

Rec'd PCT/PTO 24 SEP 2004 #2

日本国特許庁

JAPAN PATENT OFFICE

PCT/JP03/03974

28.03.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年 4月 3日

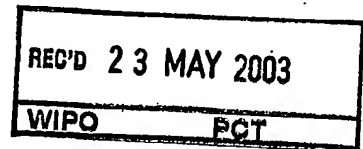
出願番号

Application Number:

特願2002-101756

[ST.10/C]:

[JP2002-101756]



出願人

Applicant(s):

株式会社エヌ・ティ・ティ・ドコモ

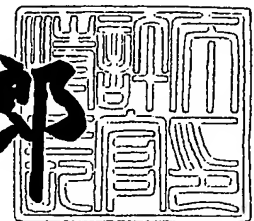
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 5月 9日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3033824

BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 DCMH130719

【提出日】 平成14年 4月 3日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 配信方法、配信システム及び端末装置

【請求項の数】 28

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ティ・ドコモ内

【氏名】 渡邊 信之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ティ・ドコモ内

【氏名】 澤田 久徳

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ティ・ドコモ内

【氏名】 西尾 英昭

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ティ・ドコモ内

【氏名】 中村 友則

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ティ・ドコモ内

【氏名】 三浦 史光

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ

・ ティ・ ティ・ ドコモ内

【氏名】 富岡 淳樹

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 配信方法、配信システム及び端末装置

【特許請求の範囲】

【請求項1】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、

前記端末装置が、前記配信システムから送信されてくるアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信されてくる前記セキュリティ記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程と

を有する配信方法。

【請求項2】 前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、

さらに、前記端末装置が、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する過程を有した

請求項1に記載の配信方法。

【請求項 3】 前記配信システムは、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保する

請求項 1 に記載の配信方法。

【請求項 4】 前記通信路は暗号化されている

請求項 3 に記載の配信方法。

【請求項 5】 前記通信路は移動通信網および専用線により実現される

請求項 3 に記載の配信方法。

【請求項 6】 前記通信路は移動通信網および暗号化された通信路により実現される

請求項 3 に記載の配信方法。

【請求項 7】 前記セキュリティ記述ファイルに内包された権限情報は資源の利用に関する制限を示す

請求項 1 に記載の配信方法。

【請求項 8】 前記資源は前記端末装置内部のハードウェア資源である

請求項 7 に記載の配信方法。

【請求項 9】 前記資源は前記端末装置外部の、当該端末装置が使用可能なハードウェア資源である

請求項 7 に記載の配信方法。

【請求項 10】 前記資源は前記端末装置内部のソフトウェア資源である

請求項 7 に記載の配信方法。

【請求項 11】 前記資源は前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源である

請求項 7 に記載の配信方法。

【請求項 12】 前記資源は、前記端末装置が使用可能なネットワーク資源である

請求項 7 に記載の配信方法。

【請求項 13】 前記権限情報は資源の利用の種類を示す

請求項 1 に記載の配信方法。

【請求項 14】 前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、

前記端末装置は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する

請求項 1 に記載の配信方法。

【請求項 15】 前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記端末装置は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する

請求項 1 に記載の配信方法。

【請求項 16】 前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記端末装置は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する

請求項 1 に記載の配信方法。

【請求項 17】 前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記端末装置が、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから前記端末装置に対して当該セキュリティ記述ファイルが時系列的に繰り返し配信され、

さらに、前記端末装置は、繰り返し配信されてくる前記セキュリティ記述フ

イルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する過程を有した

請求項 1 に記載の配信方法。

【請求項 18】 前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてこなかった場合には、前記アプリケーションの有効期限を更新しない

請求項 17 に記載の配信方法。

【請求項 19】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有し、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する

配信システム。

【請求項 20】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置と

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記アプリケーション記述ファイルを格納した情報提供サーバ装置が、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、

前記端末装置が、前記送信されてくるアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記管理サーバ装置に通知し、

前記管理サーバ装置が、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信し、

前記端末装置が、前記管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を、前記実体ファイルを格納した情報提供サーバ装置に通知し、

前記実体ファイルを格納した情報提供サーバ装置が、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する配信システム。

【請求項 2 1】 前記端末装置は移動機である

請求項 2 0 に記載の配信システム。

【請求項 2 2】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムに対し、前記アプリケーション記述ファイルの格納位置を通知するアプリケーション位置通知手段と、

前記配信システムによって送信されてくる前記アプリケーション記述ファイル

を受信するアプリケーション情報受信手段と、

前記受信したアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するセキュリティ位置通知手段と、

前記配信システムによってセキュリティが確保された状態で送信されてくる前記セキュリティ記述ファイルを受信するセキュリティ情報手段と、

前記受信したセキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を前記配信システムに通知する実体位置通知手段と、

前記配信システムによって送信されてくる前記実体ファイルを受信する実体情報受信手段と

を有した端末装置。

【請求項 23】 前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは通信事業者の秘密鍵で署名されており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されている公開鍵を用いて、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルの正当性を検証する検証手段を有し、

前記実体通知手段は、前記検証手段によって正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する

請求項 22 に記載の端末装置。

【請求項 24】 前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較する比較手段を有し、

前記実体位置通知手段は、前記比較手段によって両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する

請求項 2 2 に記載の端末装置。

【請求項 2 5】 前記セキュリティ位置通知手段は、前記アプリケーション記述ファイルに内包された、前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する

請求項 2 2 に記載の端末装置。

【請求項 2 6】 前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記セキュリティ位置通知手段が前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記セキュリティ情報受信手段は前記セキュリティ記述ファイルを時系列的に繰り返し受信し、

この繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する更新手段を有した

請求項 2 2 に記載の端末装置。

【請求項 2 7】 前記更新手段は、前記配信システムから前記セキュリティ記述ファイルが正当に送信されてこなかった場合には、前記アプリケーションの有効期限を更新しない

請求項 2 6 に記載の端末装置。

【請求項 2 8】 移動機であることを特徴とする請求項 2 2 ～ 2 7 のいずれか 1 に記載の端末装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、端末装置にアプリケーションを配信する技術に関する。

【 0 0 0 2 】

【従来の技術】

移動機の高機能化が急速に進みつつある。最近では、J a v a（登録商標）プ

プログラミング言語に従って記述されたプログラムを含むソフトウェア（以下、J a v a - A P ソフトウェアという）をネットワークを介してダウンロードし、これを実行して J a v a - A P（J a v a アプリケーション）を実現する機能を備えた移動機が開発されている。この種の移動機による J a v a - A P ソフトウェアのダウンロード手順は、まず、WWW（World Wide Web）を構成するサーバ装置から A D F（Application Descriptor File）を取得し、次いで J a r（Java Archive）ファイルを取得するという流れが通常である。

【0003】

A D F は J a r ファイルに依存した内容となっており、例えば、J a r ファイルの格納位置を示す URL（以下、パッケージ URL という）、J a r ファイルのサイズを示す情報、J a r ファイルの最終変更日時を示す情報等を必須情報として内包している。A D F を取得した移動機は、この A D F の内容を参照するとともに自機の空きメモリ容量を確認する等して、ダウンロードしようとしている J a v a - A P ソフトウェアを自機にインストール可能であるか否かを判断する。

【0004】

インストール可能と判断すると、移動機は、A D F に内包されているパッケージ URL を用いて、WWW を構成するサーバ装置から J a r ファイルを取得する。この J a r ファイルには、J a v a - A P ソフトウェアが格納されており、J a r ファイルの取得をもって J a v a - A P ソフトウェアのダウンロードは完了する。以後、移動機において、ダウンロードされた J a v a - A P ソフトウェアが起動可能に設定され、この J a v a - A P ソフトウェアのインストールが完了する。

【0005】

【発明が解決しようとする課題】

ところで、移動機内に実現される J a v a - A P の挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、J a v a - A P は、移動機内の電話帳データ等の秘匿性の高い情報を参照することができないように

なっている。このような制限の相違により、悪意をもって作成された J a v a - A P、あるいは不具合を有する J a v a - A P によって移動機内の秘匿性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができるようになっている。

【0006】

しかし、上述した厳しい挙動制限を全ての J a v a - A P に対して一律に課すだけでは、J a v a - A P の高機能化や多様化を望むユーザや I P（情報提供事業者）の意向に添うことができない。例えば、ある程度の信頼性が保証されるのであれば、移動機に格納された個人情報を参照する権限を J a v a - A P に与えてもよいと考えるユーザは少なくないと想定される。一方、I P にも、移動機に格納されている個人情報や移動機が有する多数の機能の使用を前提とした、より魅力的な J a v a - A P を提供したいという要望がある。

【0007】

これらの要望を満たす仕組みとして、移動機のユーザに対して通信サービスを提供する通信事業者等の、ユーザにとって信頼できる機関（以下、信頼機関という）が上述した挙動制限を緩和した権限を J a v a - A P に与え、この権限を移動機に通知し、移動機はこの権限に基づいて J a v a - A P の挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

【0008】

J a v a - A P ソフトウェアのダウンロード手順に上述の仕組みを適用する場合、A D F あるいは J a r ファイルに権限を示す情報を内包させるのが妥当である。とりわけ、J a r ファイルは I P により随時更新される種類のファイルであって I P が保有するのが適当であることから、信頼機関に保有させるなら A D F が妥当ということになる。

【0009】

しかしながら、A D F は J a r ファイルに依存した内容となることから、I P が手元の J a r ファイルを更新すると、信頼機関が保有している A D F の更新も必要になってくる。信頼機関は他者の関与を排するように A D F を管理すること

が必要であるから、信頼機関とIPが連携してADFを更新する作業は複雑なものとなることが懸念される。

また、Jarファイルを更新せずとも、ADFの更新が必要となることがある。例えば、IPにおいて、あるJarファイルへのアクセスが集中し、このJarファイルを他のサーバ装置へ移動する場合である。この場合、Jarファイルの格納位置が変更されるから、ADFに内包されているパッケージURLを変更する必要がある。この場合においても、上記のような懸念は当然生じ得る。

【0010】

本発明は、上述した事情に鑑みて為されたものであり、権限に応じた挙動をアプリケーションに許可する端末装置に対し、依存関係にある複数のファイルを配信することによってそのアプリケーションを実現するためのソフトウェアを配信可能な仕組みを提供することを目的としている。

【0011】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と

前記端末装置が、前記取得したアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前

記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信されてくる前記セキュリティ記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程と

を有する配信方法を提供する。

この方法によれば、配信システムが、アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、得たアプリケーション記述ファイルに内包されているセキュリティ記述ファイルの格納位置を配信システムに通知し、配信システムが、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装置が、配信システムから送信されてくるセキュリティ記述ファイルに内包されている実体ファイルの格納位置を前記配信システムに通知し、配信システムが、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

【0012】

この場合において、前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、

さらに、前記端末装置が、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する過程を有していてもよい。

【0013】

また、前記配信システムはセキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保してもよい。

この場合、前記通信路は暗号化されていてもよいし、移動通信網および専用線により実現されていてもよいし、移動通信網および暗号化された通信路により実現されていてもよい。

【0014】

また、前記セキュリティ記述ファイルに内包された権限情報は資源の利用に関する制限を示す情報であってもよい。この場合、資源は、前記端末装置内部のハードウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なハードウェア資源であってもよいし、前記端末装置内部のソフトウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源であってもよいし、前記端末装置が使用可能なネットワーク資源であってもよい。

【0015】

また、前記セキュリティ記述ファイルに内包された権限情報は資源の利用の種類を示す情報であってもよい。

【0016】

好ましい態様において、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、
前記端末装置は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する。

【0017】

好ましい態様において、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記端末装置は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する。

【0018】

好ましい態様において、前記アプリケーション記述ファイルに記述された前記

セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記端末装置は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知してもよい。

【 0 0 1 9 】

好ましい態様において、前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記端末装置が、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから前記端末装置に対して当該セキュリティ記述ファイルが時系列的に繰り返し配信され、

さらに、前記端末装置は、繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する過程を有している。

【 0 0 2 0 】

この場合において、前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてこなかった場合には、前記アプリケーションの有効期限を更新しないようにしてもよい。

【 0 0 2 1 】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有し、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知され

ると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する

配信システムを提供する。

このシステムによれば、アプリケーション記述ファイルの格納位置が通知されると、その通知元に対して当該アプリケーション記述ファイルを送信し、セキュリティ記述ファイルの格納位置が通知されると、その通知元に対してセキュリティ記述ファイルをセキュリティが確保された状態で通知元に送信し、実体ファイルの格納位置が通知されると、その実体ファイルを通知元に送信する。

【0022】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置と

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記アプリケーション記述ファイルを格納した情報提供サーバ装置が、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、

前記端末装置が、前記送信されてくるアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記管理サーバ装置に通知し、

前記管理サーバ装置が、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信し、

前記端末装置が、前記管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を、前記実体ファイルを格納した情報提供サーバ装置に通知し、

前記実体ファイルを格納した情報提供サーバ装置が、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する配信システムを提供する。

このシステムによれば、アプリケーション記述ファイルを格納した情報提供サーバ装置が、アプリケーション記述ファイルの格納位置を端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、送信されてくるアプリケーション記述ファイルに記述されているセキュリティ記述ファイルの格納位置を管理サーバ装置に通知し、管理サーバ装置が、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装置が、管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている実体ファイルの格納位置を、実体ファイルを格納した情報提供サーバ装置に通知し、実体ファイルを格納した情報提供サーバ装置が、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

【 0 0 2 3 】

この場合において、前記端末装置は移動機であれば望ましい。

【 0 0 2 4 】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムに対し、前記アプリケーション記述ファイルの格納位置を通知するアプリケーション位置通知手段と、

前記配信システムによって送信されてくる前記アプリケーション記述ファイル

を受信するアプリケーション情報受信手段と、

前記受信したアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するセキュリティ位置通知手段と、

前記配信システムによってセキュリティが確保された状態で送信されてくる前記セキュリティ記述ファイルを受信するセキュリティ情報手段と、

前記受信したセキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を前記配信システムに通知する実体位置通知手段と、

前記配信システムによって送信されてくる前記実体ファイルを受信する実体情報受信手段と

を有した端末装置を提供する。

この端末装置によれば、アプリケーション位置通知手段が、アプリケーション記述ファイルの格納位置を配信システムに通知し、アプリケーション情報受信手段が、配信システムによって送信されてくるアプリケーション記述ファイルを受信し、セキュリティ位置通知手段が、受信したアプリケーション記述ファイルに記述されているセキュリティ記述ファイルの格納位置を前記配信システムに通知し、セキュリティ情報受信手段が、配信システムによってセキュリティが確保された状態で送信されてくるセキュリティ記述ファイルを受信し、実体位置通知手段が、受信したセキュリティ記述ファイルに記述されている実体ファイルの格納位置を前記配信システムに通知し、実体情報受信手段が、配信システムによって送信されてくる実体ファイルを受信する。

【0025】

好ましくは、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは通信事業者の秘密鍵で署名されており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されている公開鍵を用いて、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルの正当性を検証する検証手段を有し、

前記実体通知手段は、前記検証手段によって正当性が検証された場合にのみ、

前記配信システムに対し前記実体ファイルの格納位置を通知する。

【0026】

好ましくは、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較する比較手段を有し、

前記実体位置通知手段は、前記比較手段によって両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する。

【0027】

好ましくは、前記セキュリティ位置通知手段は、前記アプリケーション記述ファイルに内包された、前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する。

【0028】

好ましくは、前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記セキュリティ位置通知手段が前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記セキュリティ情報受信手段は前記セキュリティ記述ファイルを時系列的に繰り返し受信し、

この繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する更新手段を有している。

【0029】

この場合において、前記更新手段は、前記配信システムから前記セキュリティ記述ファイルが正当に送信されてこなかった場合には、前記アプリケーションの

有効期限を更新しないようにしてもよい。

【0030】

なお、上記の場合において、前記端末装置は移動機であれば望ましい。

【0031】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の一形態である配信システムについて図面を参照して説明する。なお、図面において、共通する部分には同一の符号が付されている。

この配信システムは、移動通信網を管理する通信事業者（即ち信頼できる機関）が、移動機にインストール可能なJava-APソフトウェアをダウンロードするための情報を移動機のユーザへ提示し、この提示を受けたユーザが、移動機を操作して所望のJava-APソフトウェアを移動機にダウンロードおよびインストールし、移動機において起動するためのものである。

【0032】

本システムにおけるJava-APソフトウェアのダウンロードは、まず、Java-APソフトウェアの内容を説明した画面を移動機において表示した後、この移動機のユーザが所望するJava-APソフトウェアに対応したADFを移動機に配信し、次いで、上記Java-APソフトウェアに対応したSDF（セキュリティ記述ファイル）と称せられるファイルを移動機に配信し、最後にJarファイルを移動機に配信するという手順で行われる。ここで、SDFは、トラステッドAPI（Application Interface；詳しくは後述する）を使用するJava-APを移動機において実現するためのJava-APソフトウェアを移動機にダウンロードする際に必須のファイルであって、移動機内におけるJava-APソフトウェアの挙動を制限する内容が記述されたファイルである。よって、移動機は、インストールしたJava-APソフトウェアを実行するに際しては、このSDFの記述内容に従うこととなる。このSDFは、Java-APソフトウェアについて上記通信事業者とこのJava-APソフトウェアを提供するIPとの間で結ばれた契約に従って通信事業者により作成される。

【0033】

(1) 構成

図1に示されるように、この配信システムは、インターネット11に接続されたIPサーバ装置12～14と、通信事業者が移動パケット通信サービスを提供するために用いる移動パケット通信網15と、この移動パケット通信網15との間で無線パケット通信を行ってこの移動パケット通信網15を介して通信相手とパケット通信を行う移動機16と、インターネット11と移動パケット通信網15とを相互接続するゲートウェイサーバ装置17と、専用線によりゲートウェイサーバ装置17に接続された管理サーバ装置18とを有する。この配信システムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機16のみが図示されている。これと同様の理由により、3つのIPサーバ装置12～14のみが図示されている。

【0034】

以下、この配信システムの各構成要素について詳細に説明する。

(1-1) IPサーバ装置

IPサーバ装置12は第1のIPに管理されており、IPサーバ装置13および14は第1のIPと異なる第2のIPにより管理されている。IPサーバ装置12～14はWWWを構成しており、それぞれ一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。また、IPサーバ装置12は不揮発性メモリ12A、IPサーバ装置13は不揮発性メモリ13A、IPサーバ装置14は不揮発性メモリ14Aを有し、IPサーバ装置12～14はそれぞれ、TCPに従ったコネクション（以後、TCPコネクション）を通信相手との間に確立し、このコネクションを介してHTTPのGETメソッドを用いた要求メッセージを受信すると、このGETメソッドに指定されたURLで特定されるファイルを自身の不揮発性メモリから読み出し、このファイルを含むHTTPの応答メッセージを返送してこのコネクションを切断する。

【0035】

不揮発性メモリ12A、13Aおよび14Aはそれぞれハードディスク等の不揮発性メモリであり、Javaプログラミング言語を用いて作成されたプログラムを内包するJarファイルと、このJarファイルに関する情報を記述したA

D Fと、このプログラムを内包するJ a v a - A Pソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶し得る。I Pサーバ装置12～14の各々は、対応するI Pの指示に従って上記各ファイルを作成および更新する機能を備えている。

【0036】

ところで、本実施形態では、対応するS D Fが存在するJ a v a - A Pソフトウェアと、対応するS D Fが存在しないJ a v a - A Pソフトウェアとが用意されている。前者のJ a v a - A Pソフトウェアは、対応するS D Fに記述された挙動制限を受けるものであり、通信事業者がI Pとの契約に基づいて信頼性を保証したものであることから「トラステッドJ a v a - A Pソフトウェア」と呼び、後者を「非トラステッドJ a v a - A Pソフトウェア」と呼ぶ。I Pサーバ装置に格納され得るA D Fには、トラステッドJ a v a - A Pソフトウェアに対応したA D Fと、非トラステッドJ a v a - A Pソフトウェアに対応したA D Fとがある。これらのいずれもA D Fにおいても、J a v a - A Pの名称や、WWWにおけるJ a rファイルの記憶位置を示すパッケージU R Lや、J a rファイルのサイズを示す情報や、J a rファイルの最終変更日時を示す情報等の、従来からA D Fに内包されている情報が記述されている。これに加えて、トラステッドJ a v a - A Pソフトウェアに対応したA D Fは、上記のパッケージU R L等の他、図2に示されるように、トラステッドJ a v a - A Pソフトウェアを一意に識別するためのA P I Dと、J a rファイルのハッシュ値と、S D FがWWWにおいて記憶されている位置を示すU R L（以下、S D F - U R Lと呼ぶ）と、図示せぬC A（認証局）によって証明された通信事業者の公開鍵とを内包している。

【0037】

次に、説明ファイルはH T M Lに従って記述されるテキストファイルであり、移動機においてH T M Lに従って解釈されたときに、このファイルに対応するJ a v a - A Pソフトウェアをダウンロードするときにユーザにより操作されるオブジェクトとこのJ a v a - A Pソフトウェアに対応するA D FがWWWにおいて記憶されている位置を示すU R Lとが対応付けられたU I（ユーザインターフ

ェイス、以下同じ）が提供されるように記述されている。

【0038】

(1-2) ゲートウェイサーバ装置

ゲートウェイサーバ装置17は前述の通信事業者により管理されており、移動パケット通信網15とインターネット11とを接続する一般的なゲートウェイサーバ装置と同様の構成を有し、移動パケット通信網15とインターネット11と管理サーバ装置18との間で相互に通信を中継する。

【0039】

(1-3) 管理サーバ装置

管理サーバ装置18は前述の通信事業者により管理されており、WWWを構成し、一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。また、管理サーバ装置18はハードディスク等の不揮発性メモリ18Aを有し、TCPコネクションを通信相手との間に確立し、このコネクションを介してHTTPのGETメソッドを用いた要求メッセージを受信すると、このGETメソッドに指定されたURLで特定されるファイルを不揮発性メモリ18Aから読み出し、このファイルを含むHTTPの応答メッセージを返送してこのコネクションを切断する。

【0040】

不揮発性メモリ18Aに記憶されるファイルとしては、移動機16にダウンロード可能なJava-APソフトウェアを移動機16のユーザに紹介するためのリストファイル200と、複数のトラステッドJava-APソフトウェアにそれぞれ対応した複数のSDFとがある。

リストファイル200はHTMLに従って記述されたテキストファイルであり、HTMLに従って解釈された場合に、Java-APソフトウェア毎に対応した選択肢と、このJava-APソフトウェアの説明ファイルがWWWにおいて記憶されている位置を示すURLとが対応付けられたUIが提供されるように記述されている。

【0041】

SDFは、トラステッドAPソフトウェア毎に通信事業者により作成されるフ

ファイルであり、図3に示されるように、トラステッドJava-APソフトウェアを一意に識別するためのAPIDと、このトラステッドJava-APソフトウェアの移動機16における挙動制限を示すポリシー情報と、このトラステッドJava-APソフトウェアの有効期限とを内包しており、さらに、これらが通信事業者の秘密鍵によって署名されている。このSDFは、上述したADFに格納されている公開鍵で復号化されることにより、その正当性が確認されることとなる。

【0042】

SDF内のポリシー情報は、例えば図4に概念的に示されるように、トラステッドAPIの名称と、そのトラステッドAPIに対する挙動制限を示したパーミッションとが対応付けられた内容となっている。図4に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドAPIである“getPhoneList()”と移動機の状態を取得するときに必須のトラステッドAPIである“getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドAPIである“getCallHistory()”の使用が禁止されている。

【0043】

(1-4) 移動機

移動機16は、図5に示されるように、OS（オペレーティングシステム）ソフトウェア、Java-APを実行する環境を構築するためのJava-AP環境ソフトウェア、および各種ネイティブAPソフトウェア等を記憶したROM16Aと、ROM16Aからプログラムを読み出して実行するCPU16Bと、表示部16Cと、不揮発性メモリ16Dと、RAM16Eと、通信部16Fと、操作部16Gと、計時部16Hとを有し、これらは通信線によって接続されている。

【0044】

表示部16Cは、例えば液晶表示パネルやパネル駆動回路を有し、CPU16Bから供給されるデータで表される画像を表示する。

不揮発性メモリ16Dは例えばSRAM（Static Random Access Memory）

やEEPROM (Electrically Erasable and Programmable Read Only Memory) である。また、この不揮発性メモリ16Dは、WWWを構成するサーバ装置からダウンロードしたJava-APソフトウェアを記憶するために使用される。

なお、本実施形態の説明において「Java-APソフトウェア」と言う場合には、それが「トラステッドJava-APソフトウェア」であればADF、SDF及びJarファイルを含む概念とし、「非トラステッドJava-APソフトウェア」であればADF及びJarファイルを含む概念とする。

【0045】

通信部16Fは、アンテナや無線送受信部を備え、移動パケット通信網15と無線パケット通信を行うものであり、CPU16Bと移動パケット通信網15との間でパケットを中継する。また、通信部16Fは、通話のためのCODECやマイク、スピーカ等をも備えており、これによって移動機16は図示せぬ移動電話網を介して回線交換による通話を行うこともできる。

操作部16Gは操作子を備え、操作子の操作に応じた信号をCPU16Bへ供給する。

計時部16Hは現在の年月日及び時刻（以下、単に現在日時という）を計時する。なお、計時部16Hがより正確な現在日時を計時するためには、例えば移動パケット通信網15の図示せぬ基地局から制御チャネルを用いて定期的に通知される現在日時に同期させるような処理を行ってもよい。

【0046】

さて、移動機16の図示せぬ電源が投入されると、CPU16BはRAM16Eをワークエリアとし、ROM16AからOSソフトウェアに内包されているプログラムを読み出して実行する。これにより、CPU16BにはUI等を提供する機能が実現される。すなわち、CPU16BはOSソフトウェアを起動して移動機16内にて図6に示すOSを実現する。OSは操作部16Gから供給される信号とUIの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

【0047】

例えば、ユーザの指示がネイティブAPソフトウェアである通信ソフトウェアの起動を要求するものであれば、OSは通信ソフトウェアを起動して移動機16内にて通信APを実現する。この通信APを用いることで、ユーザは通話相手と通話をすることができる。

【0048】

また、ユーザの指示がネイティブAPソフトウェアである電話帳ソフトウェアの起動を要求するものであれば、OSは電話帳ソフトウェアを起動して移動機16内にて電話帳APを実現する。この電話帳APを用いることで、ユーザは、不揮発性メモリ16Dに記憶された電話帳の内容を示すデータ（以後、電話帳データという）を参照・使用・変更することができる。

【0049】

また、ユーザの指示がネイティブAPソフトウェアであるWebブラウザソフトウェアの起動を要求するものであれば、OSはWebブラウザソフトウェアを起動して移動機16内にてWebブラウザを実現する。WebブラウザはUIを提供し、このUIの状態と操作部16Gから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、この指示がユーザによって指定されたファイルをWWWから取得する旨の場合には、通信部16Fを制御してこのファイルを記憶したIPサーバ装置との間にTCPコネクションを確立し、このコネクションを介して、指定された位置を示すURLをGETメソッドに指定したHTTPの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、このコネクションを切断する。さらに、Webブラウザは、受信した応答メッセージに内包されているファイルをHTMLに従って解釈し、Webページを内包するUIを生成し、ユーザに提供する。また、ユーザの指示がJava-APソフトウェアのダウンロードを要求するものである場合には、Webブラウザは、この指示を次に述べるJAM (Java Application Manager) に通知する。より具体的には、Webページにおいて、オブジェクトタグが指定されているアンカータグで表されるアンカーが押下（クリック操作またはプレス操作）されると、Webブラウザはこのオブジェクトタグのdata属性に指定されているURLを抽出し、このURLからのJava-APソフトウ

エアのダウンロードが要求されたことをJAMに通知する。

【0050】

また、ユーザの指示がネイティブAPソフトウェアであるJAMソフトウェアの起動を要求するものであれば、OSはJAMソフトウェアを起動して移動機16内にてJAMを実現する。JAMは、移動機16にインストールされているJava-APソフトウェアの一覧をユーザに提示し、ユーザにより指定されたJava-APソフトウェアを起動する。具体的には、JAMに対するユーザの指示がJava-APソフトウェアの起動を要求するものであれば、Java-AP環境ソフトウェアが起動されて移動機16内にJava-AP環境が実現され、次に、指定されたJava-APソフトウェアが起動されてJava-AP環境内にJava-APが実現される。Java-AP環境は、移動機16のような携帯端末に適した軽量のJava仮想マシンであるKVM (K Virtual Machine) と、Java-APに対して提供されるAPI (Application Interface) とを有する。Java-APに対して提供されるAPIは、トラステッドJava-APソフトウェアによって実現されるJava-AP (以後、トラステッドJava-APという) のみに使用が許可されるトラステッドAPIと、あらゆるJava-APに使用が許可される非トラステッドAPIとに分けられる。

【0051】

次に、移動機16が備える機能について説明する。

(1-4-1) 移動機16によるJava-APソフトウェアのダウンロード機能

JAMは、Java-APソフトウェアのダウンロードを要求する指示がWebブラウザから通知されると、Java-APソフトウェアを移動機16にダウンロードしインストールする処理を行う。この処理の流れを図7に示す。

図7に示されるように、JAMは、Java-APソフトウェアのダウンロードを要求する指示がWebブラウザから通知されると(ステップS11; Yes)、

ダウンロードしようとするJava-APソフトウェアに対応するADFをIPサーバ装置12~14のいずれかから取得する(ステップS12)。具体的には

、JAMは、IPサーバ装置12～14との間にTCPコネクションを確立し、このADFの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してADFを取得した後、このTCPコネクションを切断する。そして、JAMは、応答メッセージに内包されているADFを不揮発性メモリ16Dに書き込む。

【0052】

次いで、JAMは、ダウンロードしようとしているJava-APソフトウェアを移動機16にインストール可能か否かをADFの内容に基づいて判定する（ステップS13）。ここでは、ADFに記述されていたJarファイルのサイズと、不揮発性メモリ16D内のJarファイルを記憶可能な空き容量とを比較する等の、従来と同様の基準に従って判定すればよい。

【0053】

ここで、インストール可能と判定された場合には（ステップS13；Yes）、JAMは、ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであるか否かを判定する（ステップS14）。具体的には、JAMは、ステップS12において取得したADF内にSDF-URLが記述されているか否かを確認し、記述されていれば、このJava-apソフトウェアに対応するSDFが存在する、即ち、トラステッドJava-APソフトウェアであると判定するし、その記述がなければ非トラステッドJava-APソフトウェアであると判定する。

【0054】

そして、ダウンロードしようとするJava-APソフトウェアが非トラステッドJava-APソフトウェアであると判定された場合には（ステップS14；No）、従来と同様のダウンロードおよびインストール処理が行われる（ステップS15）。

【0055】

一方、ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアと判定された場合には（ステップS14；Yes）、JAMは、このソフトウェアに対応するSDFを管理サーバ装置18から取得

する（ステップS16）。すなわち、JAMは、管理サーバ装置18との間にTCPコネクションを確立し、このコネクションを介して、ADF内に記述されているSDF-URLで示される位置に記憶されたSDFの送信を管理サーバ装置18に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してSDFを取得した後、上記コネクションを切断する。

【0056】

前述したように、トラステッドJava-APソフトウェアに対応するSDFは、APIDとポリシー情報と有効期限とを内包し、さらに通信事業者の秘密鍵により署名（暗号化）されている。そこで、JAMは、応答メッセージに内包されているSDFの署名を、既を取得しているADFから抽出された公開鍵を用いて検証し（復号し）、このSDFの正当性を判断する（ステップS17）。正当性が確認された場合（ステップS17；Yes）、JAMは、SDFを不揮発性メモリ16Dに書き込む。

【0057】

次いで、JAMは、SDFに内包されているAPIDと、既を取得しているADFに内包されていたAPIDとを比較し、両者が一致するか否かを判定する（ステップS18）。

両者が一致すると判定された場合には（ステップS18；Yes）、JAMは、Jarファイルを取得する（ステップS19）。具体的には、JAMは、ADFに内包されているパッケージURLで特定されるJarファイルを記憶したIPサーバ装置12～14のいずれかとの間にTCPコネクションを確立し、このJarファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してJarファイルを取得し、このTCPコネクションを切断する。

【0058】

次に、JAMは、取得したJarファイルに対するハッシュ値を算出する（ステップS20）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機16で使用するハッシュ関数とADFに含まれるハッシュ値の算出時に使用されるハッシュ関数とは一致していなければならない。実際には、移動機16

で使用されるハッシュ関数を用いて、トラステッド J a v a - A P ソフトウェアを提供する I P がハッシュ値を算出して A D F を生成することになる。

【 0 0 5 9 】

J A M は、算出したハッシュ値と A D F から抽出したハッシュ値とを比較し、両者が一致した場合には（ステップ S 2 1 ; Y e s）、取得した J a r ファイルを不揮発性メモリ 1 6 D に書き込み、トラステッド J a v a - A P ソフトウェアのインストールに係る各種処理を行い（ステップ S 2 2）、インストールに成功した旨をユーザに通知する（ステップ S 2 3）。

以降、J A M は、トラステッド J a v a - A P ソフトウェアを実行するに際し、トラステッド J a v a - A P の挙動を監視し、トラステッド A P I の使用を制限するが、この制限は不揮発性メモリ 1 6 D に記憶される S D F 内のポリシー情報に従って行われることとなる。

【 0 0 6 0 】

なお、J a v a - A P ソフトウェアをインストール不可能と判断された場合（ステップ S 1 3 ; N o）、S D F が正当でないと判断した場合（ステップ S 1 7 ; N o）、S D F が有する A P I D と A D F が有する A P I D が不一致の場合（ステップ S 1 8 ; N o）、算出したハッシュ値と A D F が有するハッシュ値とが不一致の場合（ステップ S 2 1 ; N o）には、J A M は、インストールに失敗した旨をユーザに通知するとともに、移動機 1 6 の状態をステップ S 1 1 以前の状態に戻す。

【 0 0 6 1 】

（ 1 - 4 - 2 ） 移動機 1 6 による S D F の更新機能

ところで、トラステッド J a v a - A P ソフトウェアは、対応する S D F に内包されていた有効期限が経過するまでは移動機 1 6 によって実行可能である。この有効期限を更新する場合には、移動機 1 6 は、管理サーバ 1 8 から新たに S D F を取得する必要がある。そこで、以下では、J A M が、S D F 内の有効期限が到来する度にその有効期限を更新する場合の処理について、図 8 に示すフローを参照しながら説明する。

【 0 0 6 2 】

図 8 に示されるように、J A M は、移動機 1 6 内の計時部 1 6 H によって計時される現在日時と、今までに取得した全ての S D F からそれぞれ抽出して不揮発性メモリ 1 6 D に記憶した複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している（ステップ S 3 1）。

【 0 0 6 3 】

いずれか 1 つでも有効期限が到来すると（ステップ S 3 1 ; Y e s）、J A M は、有効期限が到来した J a v a - A P ソフトウェアの名称とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部 1 6 C に表示してユーザの操作があるまで待機する。

ユーザが有効期限を更新することを指示する操作を行うと、J A M はこの指示内容を解釈し（ステップ S 3 2 ; Y e s）、この有効期限を更新すべき J a v a - A P ソフトウェアに対応する S D F を管理サーバ装置 1 8 から取得する（ステップ S 3 3）。具体的には、J A M は、不揮発性メモリ 1 6 D の記憶内容を参照し、有効期限を更新すべき J a v a - A P ソフトウェアの A P I D を内包した A D F に内包されている S D F - U R L を抽出し、この S D F - U R L で示される位置に記憶された S D F の送信を管理サーバ装置 1 8 に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信して S D F を取得した後、上記コネクションを切断する。

【 0 0 6 4 】

次いで、J A M は、上記 S D F - U R L を用いて S D F を取得できたか否かを判断する（ステップ S 3 4）。ここで、S D F を取得できない場合とは、何らかの事情で J a v a - A P ソフトウェアの使用を中断或いは中止させたいという理由から、通信事業者が、管理サーバ装置 1 8 において上記の S D F - U R L によって示される位置に S D F を記憶させていないことを意味している。その事情とは、例えば、I P の都合によって J a v a - A P ソフトウェアの使用を中止或いは中断させたい場合（例えば、ユーザが一定期間だけ試用できるソフトウェアを配信するような場合）や、I P と通信事業者との間で締結されていた契約が失効した場合等である。

【 0 0 6 5 】

さて、JAMは、SDFの取得に成功すると（ステップS34；Yes）、SDFの署名を、既に取得しているADFに内包されている公開鍵を用いて検証し（復号し）、このSDFの正当性を判断する（ステップS35）。

【0066】

正当性が確認されると（ステップS35；Yes）、JAMは、SDFに内包されているAPIDと、既に取得済みのADFに内包されているAPIDとを比較し、両者が一致するか否かを判定する（ステップS36）。両者が一致すると判定された場合には（ステップS36；Yes）、JAMは、取得したSDFを不揮発性メモリ16Dに既にかき込まれている以前のSDFに上書きし、これにより有効期限を更新する。

【0067】

なお、ユーザの操作により有効期限を更新しないと判断された場合（ステップS32；No）、SDFを取得できなかった場合（ステップS34；No）、SDFが正当でないと判断した場合（ステップS35；No）、SDFが有するAPIDとADFが有するAPIDが不一致の場合（ステップS36；No）、JAMは、有効期限を更新しない旨をユーザに通知するとともに、移動機16の状態をステップS31以前の状態に戻す。

【0068】

（2）動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、TCPコネクションの確立および切断動作についてはHTTPにおける一般的な動作となることから、それらの説明を省略する。また、前述のOS、Webブラウザ、JAM、Java-AP、ネイティブAP等が行う動作は移動機16の動作となることから、以降の説明では、動作の主体を移動機16とする。

【0069】

また、図9に示されるように、管理サーバ装置18の不揮発性メモリ18Aには、リストファイル200とSDF204が記憶されているものとする。これらはIPサーバ装置13およびIPサーバ装置14を管理するIPと管理サーバ装

置 18 を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されている。

これらのうち、リストファイル 200 は、移動機 16 において解釈・実行されると図 10 に示されるリストページ 201 を提供するように記述されている。また、リストファイル 200 は、リストページ 201 を構成する選択肢 201A が押下されると（クリックまたはプレスされると）、後述の説明ファイル 202 の URL（“http://www.main.bbb.co.jp/ghi.html”）を GET メソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル 200 は、リストページ 201 を構成する選択肢 201B が押下されると（クリックまたはプレスされると）、後述の説明ファイル 207 の URL（“http://www.ccc.co.jp/jkl.html”）を GET メソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

【0070】

また、SDF 204 は、API D として “0001”、ポリシー情報として図 4 に示される内容の情報、有効期限として “2002 年 10 月 1 日午前 10 時” を内包しており、これらは通信事業者の秘密鍵を用いて署名されている。

【0071】

また、IP サーバ装置 12 の不揮発性メモリ 12A には、「詰め将棋」なる名称の Java-AP ソフトウェア（これを、本動作例では、第 1 の非トラステッド Java-AP ソフトウェアとする）に対応する説明ファイル 211、ADF 213 および Jar ファイル 214 が記憶されているものとする。これらは IP サーバ装置 12 を管理する IP によって作成されている。これらのうち、説明ファイル 211 の内容は図 11 に示される通りであり、移動機 16 において解釈・実行されると図 12 に示される説明ページ 212 を提供するように記述されている。また、ADF 213 はパッケージ URL として Jar ファイル 214 の URL（“http://www.ccc.co.jp/shogi.jar”）を内包している。

【0072】

また、IP サーバ装置 12 の不揮発性メモリ 12A には、「星占い」なる名称の Java-AP ソフトウェア（これを、本動作例では、第 2 の非トラステッド

J a v a - A P ソフトウェアとする) に対応する説明ファイル 207、ADF 209 および J a r ファイル 210 が記憶されているものとする。これらは I P サーバ装置 12 を管理する I P によって作成されている。これらのうち、説明ファイル 207 の内容は図 13 に示される通りであり、移動機 16 において解釈・実行されると図 14 に示される説明ページ 208 を提供するように記述されている。また、ADF 209 はパッケージ URL として J a r ファイル 210 の URL (“http://www.ccc.co.jp/horoscope.jar”) を内包している。

なお、上述した第 1 の非トラステッド J a v a - A P ソフトウェアと第 2 の非トラステッド J a v a - A P ソフトウェアの違いは、後者に関連する情報がリストファイル 200 に登録されているのに対し、前者に関連する情報が登録されていない点にある。

【0073】

また、I P サーバ装置 13 の不揮発性メモリ 13A には、「電話帳ビューア」なる名称の J a v a - A P ソフトウェア (これを、本動作例ではトラステッド J a v a - A P ソフトウェアとする) に対応する説明ファイル 202、ADF 205 および J a r ファイル 206 が記憶されているものとする。これらは I P サーバ装置 13 および I P サーバ装置 14 を管理する I P によって作成されている。これらのうち、説明ファイル 202 の内容は図 15 に示される通りであり、移動機 16 において解釈・実行されると図 16 に示される説明ページ 203 を提供するように記述されている。ADF 205 は、A P I D として “0001”、ハッシュ値として J a r ファイル 206 のハッシュ値、パッケージ URL として J a r ファイル 206 の URL (“http://www.main.bbb.co.jp/viewer.jar”)、S D F - URL として S D F 204 の URL (“http://www.aaa.co.jp/viewer.sdf”)、及び通信事業者の公開鍵を内包している。また、移動機 16 は上述の各 J a v a - A P ソフトウェアをインストール可能な状態にあるものとする。

【0074】

(2-1) インストール動作

まず、J a v a - A P ソフトウェアを移動機 16 にインストールする場合の動作例について、上述した J a v a - A P ソフトウェア毎に説明する。

(2-1-1) 第1の非トラステッドJava-APソフトウェア

第1の非トラステッドJava-APソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル211の取得を試みることから始まる。これにより、移動機16では、説明ファイル211のURL（“http://www.ccc.co.jp/mno.html”）をGETメソッドのパラメータとして含む要求メッセージtm12が生成される。この要求メッセージtm12は、図17に示されるように、移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm12の内容に対応して説明ファイル211を内包した応答メッセージtm13が生成される。この応答メッセージtm13はIPサーバ装置12から送信され移動機16により受信される。移動機16では、ユーザに対して、説明ファイル211の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図12に示すような説明ページ212が表示される。

【0075】

この説明ページ212を視たユーザが、説明ページ212内のアンカー212Aが押下されるよう移動機16を操作すると、移動機16では、図11の説明ファイル211に記述されたアンカータグ（“<A”で始まるタグ）のijam属性に指定されている値がid属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのdata属性に指定されているURL（“http://www.ccc.co.jp/shogi.jam”）が抽出され、このURLで特定されるADF213の送信を要求する内容の要求メッセージtm16が生成される。この要求メッセージtm16は移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm16の内容に対応してADF213を内包した応答メッセージtm17が生成される。この応答メッセージtm17はIPサーバ装置12から送信され移動機16により受信される。

【0076】

移動機16では、ADF213の内容に基づいて第1の非トラステッドJava-APソフトウェアをインストール可能か否かが判定される。前述のように、

移動機 16 は非トラステッド J a v a - A P ソフトウェアをインストール可能な状態にあるから、移動機 16 では第 1 の非トラステッド J a v a - A P ソフトウェアをインストール可能と判定される。

【0077】

次に、移動機 16 では、A D F 2 1 3 が不揮発性メモリ 16 D に書き込まれる。また、移動機 16 では、A D F 2 1 3 からパッケージ URL (“http://www.cc.co.jp/shogi.jar”) が抽出され、このパッケージ URL で特定される J a r ファイル 2 1 4 の送信を要求する内容の要求メッセージ t m 1 8 が生成される。この要求メッセージ t m 1 8 は移動機 16 から送信され I P サーバ装置 1 2 により受信される。

I P サーバ装置 1 2 では、この要求メッセージ t m 1 8 の内容に対応して J a r ファイル 2 1 4 を内包した応答メッセージ t m 1 9 が生成される。この応答メッセージ t m 1 9 は I P サーバ装置 1 2 から送信され移動機 16 により受信される。移動機 16 では J a r ファイル 2 1 4 が不揮発性メモリ 16 D に起動可能な状態で書き込まれ、これにより、第 1 の非トラステッド J a v a - A P ソフトウェアのインストールが完了する。

なお、移動機 16 において第 1 の非トラステッド J a v a - A P ソフトウェアをインストール可能ではないと判断された場合、移動機 16 の状態は A D F 2 1 3 の取得を開始する前の状態に戻る。

【0078】

(2-1-2) 第 2 の非トラステッド J a v a - A P ソフトウェアの

第 2 の非トラステッド J a v a - A P ソフトウェアのインストール動作は、ユーザが移動機 16 を操作し、説明ファイル 207 またはリストファイル 200 の取得を試みることから始まる。説明ファイル 207 の取得を試みることから始まる動作はリストファイル 200 の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル 200 の取得を試みることから始まる動作のみについて説明する。

【0079】

図 18 に示されるように、移動機 16 では、リストファイル 200 の URL (

“http://www.aaa.co.jp/def.html”) をGETメソッドのパラメータとして含む要求メッセージtm20が生成される。この要求メッセージtm20は移動機16から送信され管理サーバ装置18により受信される。

管理サーバ装置18では、この要求メッセージtm20の内容に対応してリストファイル200を内包した応答メッセージtm21が生成される。この応答メッセージtm21は管理サーバ装置18から送信され移動機16により受信される。移動機16では、応答メッセージtm21の受信を契機として、応答メッセージtm21内のリストファイル200がHTMLに従って解釈され、移動機16のユーザに対して、リストファイル200の内容に応じたUIが提供される。この結果、移動機16の表示部16Cには、例えば図10に示すようなリストページ201が表示される。

【0080】

このリストページ201を視たユーザが、リストページ201内の選択肢201Bが押下されるように移動機16を操作すると、移動機16では、選択肢201Bに対応付けられているURL (“http://www.ccc.co.jp/jkl.html”) をGETメソッドのパラメータとして含む要求メッセージtm22が生成される。この要求メッセージtm22は移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm22の内容に対応して説明ファイル207を内包した応答メッセージtm23が生成される。この応答メッセージtm23はIPサーバ装置12から送信され移動機16により受信される。移動機16では、ユーザに対して、説明ファイル207の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図14に示すような説明ページ208が表示される。

【0081】

この説明ページ208を視たユーザが、説明ページ208内のアンカー208Aが押下されるよう移動機16を操作すると、移動機16では、図13の説明ファイル207に記述されたアンカータグ (“<A” で始まるタグ) のijam属性に指定されている値がid属性に指定されているオブジェクトタグ (“<OBJECT

”で始まるタグ)が特定され、このオブジェクトタグのdata属性に指定されているURL (“http://www.ccc.co.jp/horoscope.jam”)が抽出され、このURLで特定されるADF209の送信を要求する内容の要求メッセージtm26が生成される。この要求メッセージtm26は移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm26の内容に対応してADF209を内包した応答メッセージtm27が生成される。この応答メッセージtm27はIPサーバ装置12から送信され移動機16により受信される。

【0082】

移動機16では、ADF209の内容に基づいて第2の非トラステッドJava-Apソフトウェアをインストール可能か否かが判定される。前述のように、移動機16は第2の非トラステッドJava-Apソフトウェアをインストール可能な状態にあるから、移動機16では非トラステッドJava-Apソフトウェアをインストール可能と判定される。

【0083】

次に、移動機16では、ADF209が不揮発性メモリ16Dに書き込まれる。また、移動機16では、ADF209からパッケージURL (“http://www.ccc.co.jp/horoscope.jar”)が抽出され、このパッケージURLで特定されるJarファイル210の送信を要求する内容の要求メッセージtm28が生成される。この要求メッセージtm28は移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm28の内容に対応してJarファイル210を内包した応答メッセージtm29が生成される。この応答メッセージtm29はIPサーバ装置12から送信され移動機16により受信される。移動機16ではJarファイル210が不揮発性メモリ16Dに起動可能な状態で書き込まれ、これにより、第2の非トラステッドJava-Apソフトウェアのインストールが完了する。

なお、移動機16において、第2の非トラステッドJava-Apソフトウェアをインストール可能ではないと判断された場合、移動機16の状態は、ADF

209の取得を開始する前の状態に戻る。

【0084】

(2-1-3) トラステッドJava-APソフトウェア

トラステッドJava-APソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル202またはリストファイル200の取得を試みることから始まる。説明ファイル202の取得を試みることから始まる動作はリストファイル200の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル202の取得を試みることから始まる動作についての説明を省略する。

【0085】

図19に示されるように、リストファイル200の取得を試みることから始まる動作において、移動機16が応答メッセージtm21を受信し、例えば図10に示すようなリストページ201が表示されるまでは図18に示す動作と同一の動作が行われる。このリストページ201を視たユーザが、リストページ201内の選択肢201Aが押下されるように移動機16を操作すると、移動機16では、選択肢201Aに対応付けられているURL (“http://www.main.bbb.co.jp/ghi.html”) をGETメソッドのパラメータとして含む要求メッセージtm32が生成される。この要求メッセージtm32は移動機16から送信されIPサーバ装置13により受信される。

IPサーバ装置13では、この要求メッセージtm32の内容に対応して説明ファイル202を内包した応答メッセージtm33が生成される。この応答メッセージtm33はIPサーバ装置13から送信され移動機16により受信される。移動機16では、ユーザに対して、説明ファイル202の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図16に示すような説明ページ203が表示される。

【0086】

この説明ページ203を視たユーザが、説明ページ203内のアンカー203Aが押下されるよう移動機16を操作すると、移動機16では、図15の説明ファイル202に記述されたアンカータグ (“<A” で始まるタグ) のijam属性

に指定されている値が `id` 属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグの `data` 属性に指定されている URL（“<http://www.main.bbb.co.jp/viewer.jam>”）が抽出され、この URL で特定される ADF205 の送信を要求する内容の要求メッセージ `tm34` が生成される。この要求メッセージ `tm34` は移動機 16 から送信され IP サーバ装置 13 により受信される。IP サーバ装置 13 では、この要求メッセージ `tm34` の内容に対応して ADF205 を内包した応答メッセージ `tm35` が生成される。この応答メッセージ `tm35` は IP サーバ装置 13 から送信され、ゲートウェイサーバ装置 17 及び移動パケット通信網 15 を介して移動機 16 により受信される。

【0087】

移動機 16 において、ADF205 は不揮発性メモリ 16D に書き込まれ、ADF205 の内容に基づいてトラステッド Java-AP ソフトウェアをインストール可能か否かが判定される。前述のように、移動機 16 はトラステッド Java-AP ソフトウェアをインストール可能な状態にあるから、移動機 16 ではトラステッド Java-AP ソフトウェアをインストール可能と判定される。

【0088】

そして、移動機 16 では、ADF205 に内包されている SDF-URL “<http://www.aaa.co.jp/viewer.sdf>” で特定される SDF204 の送信を要求する内容の要求メッセージ `tm36` が生成される。この要求メッセージ `tm36` は移動機 16 から送信され管理サーバ装置 18 により受信される。

管理サーバ装置 18 では、この要求メッセージ `tm36` の内容に対応して SDF204 を内包した応答メッセージ `tm37` が生成される。この応答メッセージ `tm37` は管理サーバ装置 18 から送信されゲートウェイ装置 17 及び移動パケット通信網 15 を介して移動機 16 により受信される。ここで、管理サーバ装置 18 とゲートウェイサーバ装置 17 との間の通信路は専用線であり、ゲートウェイサーバ装置 17 はセキュリティの確保された移動パケット通信網 15 に直接的に接続されていることから、移動機 16 に受信されるまでに SDF204 が改竄される虞は無い。

【0089】

さらに、移動機16では、ADF205に内包されている公開鍵を用いてSDF204の正当性が判断される。前述のように、ADF205に内包されている公開鍵はSDF204への署名の際に用いた秘密鍵と対応していることから、管理サーバ装置18内においてSDF204の内容が変更されていない限り、SDF204が正当であると判断される。

【0090】

SDF204が正当であると判断されると、移動機16では、ADF205に内包されているAPIDとSDF204に内包されているAPIDとが比較される。前述のように、IPサーバ装置13におけるADF205にはSDF204内のAPIDと一致するAPIDが記述されるように定められていることから、記述ミス等が無い限り、ADF205に内包されているAPIDとSDF204に内包されているAPIDは一致する。次いで、移動機16では、SDF204が不揮発性メモリ16Dに書き込まれる。

【0091】

次に、移動機16では、ADF205からパッケージURL（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージURLで特定されるJarファイル206の送信を要求する内容の要求メッセージtm38が生成される。この要求メッセージtm38は移動機16から送信されIPサーバ装置13により受信される。

IPサーバ装置13では、この要求メッセージtm38の内容に対応してJarファイル206を内包した応答メッセージtm39が生成される。この応答メッセージtm39はIPサーバ装置13から送信され移動機16により受信される。

【0092】

次に、移動機16ではJarファイル206と所定のハッシュ関数とを用いてハッシュ値が算出され、このハッシュ値とADF205に内包されているハッシュ値とが比較される。前述のように、ADF205にはこのADF205に対応するJarファイルのハッシュ値が記述されるように定められていることから、

記述ミス等がない限り、両ハッシュ値は一致する。

両ハッシュ値が一致すると、移動機16では、Jarファイル206が不揮発性メモリ16Dに起動可能な状態で書き込まれ、これにより、トラステッドJava-APソフトウェアのインストールが完了する。

【0093】

なお、移動機16においてSDF204が正当でないと判断された場合や、ADF205に内包されているAPIDとSDF204に内包されているAPIDが不一致の場合、トラステッドJava-APソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とADF205に内包されているハッシュ値とが不一致の場合には、移動機16の状態はADF205の取得を開始する前の状態に戻る。

【0094】

(2-2) Java-APソフトウェアが起動されている時の移動機16の挙動
次に、上述の各々のJava-APソフトウェアが起動されている時の移動機16の挙動について説明する。

(2-2-1) 非トラステッドJava-APソフトウェアの挙動

上述したインストール動作により移動機16にインストールされた非トラステッドJava-APソフトウェア(第1の非トラステッドJava-APソフトウェア(詰め将棋)及び第2の非トラステッドJava-APソフトウェア(星占い)の双方を含む)が、JAMが実現された移動機16において起動され、このソフトウェアに対応した機能(以後、非トラステッドJava-AP)が移動機16内に実現されたときの移動機16の挙動について説明する。

【0095】

非トラステッドJava-APが使用しようとするAPIが非トラステッドAPIの場合、前述したように非トラステッドAPIはあらゆるJava-APの使用が許可されているから、この場合のAPIの使用はJAMにより許可されることとなる。したがって、非トラステッドJava-APはこの非トラステッドAPIを使用することができる。

また、非トラステッドJava-APが使用しようとするAPIがトラステッ

ドAPIの場合、JAMはこのJava-APに対応するSDFが不揮発性メモリ16Dに記憶されているか否かを調べる。ここでは、そのようなSDFは不揮発性メモリ16Dに記憶されていないから、JAMは非トラステッドJava-APによるこのAPIの使用を禁止する。したがって、非トラステッドJava-APはトラステッドAPIを使用することができない。

【0096】

(2-2-2) トラステッドJava-APソフトウェアの挙動

移動機16にインストールされたトラステッドJava-APソフトウェア（電話帳ビューワ）が、JAMが実現された移動機16において起動され、このソフトウェアに対応した機能が移動機16内に実現されたときの移動機16の挙動について説明する。

トラステッドJava-APが使用しようとするAPIが非トラステッドAPIの場合、前述したように、このAPIの使用はJAMによって当然許可される。したがって、トラステッドJava-APはこの非トラステッドAPIを使用することができる。

トラステッドJava-APが使用しようとするAPIがトラステッドAPIの場合、このJava-APに対応するSDFが不揮発性メモリ16Dに記憶されているので、このAPIの使用はJAMによって許可され得るが、そのトラステッドJava-APの挙動はSDF内のポリシー情報に依存する。以下、使用するAPI毎にその挙動について説明する。

【0097】

(2-2-2-1) getPhoneList()

“getPhoneList()”はトラステッドAPIであるから、このAPIの使用の可否は、不揮発性メモリ16Dに記憶されているSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図4に示される通りであることから、“getPhoneList()”の使用がJAMにより許可される。したがって、トラステッドJava-AP（電話帳ビューワ）は“getPhoneList()”を使用することができる。つまり、このトラステッドJava-APは電話帳データを読み出すことができる。

【0098】

(2-2-2-2) getCallHistory()

“getCallHistory()”はトラステッドAPIであるから、このAPIの使用の可否はSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図4に示される通りであることから、“getCallHistory()”の使用がJAMにより禁止される。したがって、トラステッドJava-AP（電話帳ビューワ）は“getCallHistory()”を使用することができない。つまり、このトラステッドJava-APは発着信履歴データを読み出すことができない。

【0099】

(2-3) トラステッドJava-APソフトウェアの有効期限更新時の動作

次に、トラステッドJava-APソフトウェアの有効期限を更新する動作例について説明する。以下の説明においては、図9において、管理サーバ装置18内においてSDF204がSDF204aに更新されているものとする。ただし、その更新内容は、有効期限が“2002年10月1日午前10時”から“2003年1月1日午前10時”に変更されたということのみであり、SDF204とSDF204aの記憶位置やそのファイル名、署名に用いた秘密鍵等は一切変更されていないものとする。

【0100】

移動機16は、計時部16Hによって計時される現在日時と、今までに取得した全てのSDFに内包されている複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している。ここで、計時部16Hによって計時される現在日時が2002年10月1日午前10時となったとき、APID“0001”に対応するトラステッドJava-APソフトウェア（電話帳ビューワ）の有効期限が到来することとなり、これによって、図20に示す動作が開始される

【0101】

まず、移動機16は、図21に示すように、有効期限が到来したトラステッドJava-APソフトウェアの名称“電話帳ビューワ”とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部16cに

表示してユーザの操作があるまで待機する。

ここで、ユーザが有効期限を更新することを指示する操作を行うと、移動機16はこの指示内容を解釈し、APIID“0001”を内包したADFに内包されているSDF-URL (“http://www.aaa.co.jp/viewer.sdf”)をGETメソッドのパラメータとして含む要求メッセージtm41を生成する。この要求メッセージtm41は移動機16から送信され管理サーバ装置18により受信される。

管理サーバ装置18では、この要求メッセージtm41の内容に対応してSDF204aを内包した応答メッセージtm42が生成される。この応答メッセージtm42は管理サーバ装置18から送信され移動機16により受信される。

【0102】

一方、移動機16は、上記SDF-URLを用いてSDF204aを取得できたか否かを判断する。ここでは取得に成功することを想定しているので処理は次に進み、移動機16は、SDF204aの署名を、既に取得しているADF205に内包されている公開鍵を用いて検証し（復号し）、このSDF204aの正当性を判断する。正当性が確認されると（ステップS35；Yes）、移動機16は、SDF204aから抽出したAPIIDと既に取得済みのADF205に内包されていたAPIIDとを比較し、両者が一致するか否かを判定する。

ここでは両者が一致するはずなので、移動機16は、不揮発性メモリ16Dに記憶されているSDF203をSDF204aで上書きし、これにより、トラステッドJava-APソフトウェア（電話帳ビューワ）の有効期限が“2002年10月1日午前10時”から“2003年1月1日午前10時”に更新される。

なお、ユーザの操作により有効期限を更新しないと判断された場合、SDFを取得できなかった場合、SDFが正当でないと判断した場合、SDFが有するAPIIDとADFが有するAPIIDが不一致の場合、JAMは、有効期限を更新しない旨をユーザに通知するとともに、移動機16の状態をSDF203aを取得する以前の状態に戻す。

【0103】

（2-4）トラステッドJava-APソフトウェアの変更後の動作

次に、IPサーバ装置13およびIPサーバ装置14を管理するIPがトラステッドJava-APソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、トラステッドJava-APソフトウェアの改善等を目的としたJarファイル206の内容の変更と、IPサーバ装置13の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、IPサーバ装置13およびIPサーバ装置14を管理するIPは、図22に示すように、変更後のJarファイル206（以後、Jarファイル215）をIPサーバ装置14の不揮発性メモリ14Aに記憶させ、このJarファイル215に対応するようにADF205の内容を変更してADF216としている。変更後のトラステッドJava-APソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置18を管理する通信事業者が行うべき作業は存在しない。つまり、通信事業者はリストファイル200やSDF204を変更する必要はない。

【0104】

このような変更の後のトラステッドJava-APソフトウェアのインストール動作は、図23に示す通りとなる。この図に示す動作が図19に示す動作と相違し始めるのは、移動機16がJarファイルを要求する時点からである。なお、両図において、応答メッセージtm47は応答メッセージtm37、要求メッセージtm48は要求メッセージtm38、応答メッセージtm49は応答メッセージtm39に対応している。

即ち、図23において図19に示す動作と本質的に異なるのは、ADF216およびJarファイル215が処理の対象となる点と、ADF216に内包されているパッケージURL（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるJarファイル215の送信を要求する内容の要求メッセージtm48が移動機16にて生成される点と、この要求メッセージtm48が移動機16から送信されIPサーバ装置14により受信される点と、IPサーバ装置14においてJarファイル215を内包した応答メッセージtm49が生成される点と、この応答メッセージtm49がIPサーバ装置14から送信され移動機16により受信される点のみである。

【0105】

以上説明したように、移動機16においては、ダウンロードしたSDFに含まれるポリシー情報の内容に応じた挙動がこのSDFに対応するトラステッドJava-A Pソフトウェアに許可され、ポリシー情報の内容に含まれていない挙動は許可されない。このポリシー情報は管理サーバ装置18からセキュリティが確保された上で移動機16へ送信されるから、ポリシー情報が第三者により改竄される虞もなく、これにより、トラステッドJava-A Pの信頼性が確保される。また、ユーザから視れば、従来通りの非トラステッドJava-A Pの他に、上記のような、より自由な挙動が許可されたトラステッドJava-A Pを利用可能となり、非常に便利である。

【0106】

なお、上述の配信システムにおいては、移動機16に対し、ADF、SDF、Jarファイルという順序で各種ファイルの配信を行っていたが、このような順序で配信することにより、以下のような効果が生ずる。

既に説明したように、Java-A Pソフトウェア（ADF及びJarファイル）はIPによって設計・作成され、各々のIPがインターネット上に開設している専用サイト（図1のIPサーバ装置12～14）において、一般ユーザに公開されている。従って、ユーザはまず、IPの専用サイトにアクセスし、そこで、様々なJava-A Pソフトウェアの解説ページを参照してそのソフトウェアをダウンロードをするか否かを判断するのが普通である。そして、ユーザはJava-A Pソフトウェアをダウンロードしようと判断すると、そのダウンロード処理を指示する操作を行う必要があるが、そのために上記の解説ページには次にダウンロードすべきファイルのURLがアンカータグによって埋め込まれているのが普通である。このとき、IPの立場から視れば、解説ページにADFのURLを埋め込むのが最も手間がかからない。なぜなら、ADFはIPの管理下にあるので、そのADFのURLはIPによって常に把握できているからである。これに対し、解説ページにSDFのURLを埋め込むとなると、IPは通信事業者に問い合わせをする等して、URLの正誤の確認処理を絶えず欠かさないようにしなければならない。よって、ADF、SDF、Jarファイルという順序で各

種ファイルの配信を行うことは非常に有意義である。

【0107】

また、上記の順序は、エヌティティドコモ社のiモード（登録商標）において現在実施されているJava-APソフトウェアのバージョンアップ処理を考慮した場合にも利点がある。現状のiモードのサービス仕様においては、ユーザによってバージョンアップを要求する操作がなされると、移動機は、まず、ADFに記述された内容を参照し、ADFに記述されたパッケージURLに基づいて、バージョンアップ後のJarファイルを取得するようになっている。即ち、バージョンアップ時には、まずADFを参照してから、その後にダウンロード処理に移行するようになっている。この点を考慮すると、本実施形態の配信システムにおけるバージョンアップ時においても、まずADFを参照し、そのADFに記述されているSDF-URLに基づいてSDFを取得した後、Jarファイルを取得するというように、まずADFの参照から一連の処理を開始すると、それ以降は、SDF→Jarファイルという通常のダウンロードと同じ流れで処理を行うことができ、現状のサービス仕様をあまり変更しないで済む。これに対し、仮にSDF、ADF、Jarファイルという順序で各種ファイルをダウンロードすることが定義付けられている場合、バージョンアップしようとした場合、ADFを参照からダウンロード処理を開始すると、SDFを取得することなくJarファイルの取得処理にまで至ってしまう。SDFは、バージョンアップ時に書き換えられることは十分にあり得るので、SDFが無いとセキュリティ上で不都合が生ずるおそれがある。以上のような観点からも、ADF、SDF、Jarファイルという順序で各種ファイルの配信を行うことは有意義である。

【0108】

(3) 変形例

本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてSDFとADFの作成者との対応関係の正当性を確認するようにした。しかし、これに限らず、SDFとADFの作成者との対応関係の正当性が確認でき

る方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、SDFに公開鍵を内包させず、IPサーバ装置においてはADFに対する秘密鍵を用いた署名を行わず、かつ移動機においてはこの確認処理を省略する、という形態とし、移動機およびIPサーバ装置における処理量や、移動機と管理サーバ装置およびIPサーバ装置との間の通信量を低減するようにしてもよい。

【0109】

また、上述した配信システムでは、Jarファイルのハッシュ値をこのJarファイルに対応するADFに内包させる一方、移動機においてJarファイルのハッシュ値を生成し、これら両者を比較してJarファイルとADFとの対応関係の正当性を確認するようにしていた。しかし、これに限らず、JarファイルとADFとの対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、ADFにハッシュ値を内包させずにこの確認処理を省略する形態とし、移動機およびIPサーバ装置における処理量や移動機とIPサーバ装置との間の通信量を低減するようにしてもよい。

【0110】

また、上述した配信システムでは、トラステッドJava-APに固有のAPIDを使用してSDFとADF（およびJarファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドJava-APを提供する情報提供事業者固有のCIDを用いてSDFとADF（およびJarファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、APIDやCIDを用いた判定を省略するようにしてもよい。

【0111】

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、IPアドレスを用いてサーバを指定するようにしてもよい。

【0112】

また、移動機において、ADFに内包されているSDF-URLのうちのドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、SDFを正当と認める態様としてもよい。この場合、予め設定された文字列と異なるときは、移動機16は、SDF取得に失敗した旨を表示し、管理サーバ18にSDFを要求せずに処理を終了することとなる。

また、この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のROMまたは不揮発性メモリに予め格納されることになる。ROMに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

【0113】

また、上述した配信システムでは、SDFの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がSDFを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、SDFを暗号化した後に配信し、移動機においてSDFを復号するようにすれば、ある程度のセキュリティを確保してSDFを配信することができる。

【0114】

上述した配信システムでは、HTTPに従ってファイルを送受するようにしたが、HTTPSを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

【0115】

また、上述した配信システムにおいて、信頼できる機関がIPとなってよいこと、すなわち、管理サーバ装置がIPサーバ装置を兼ねるようにしてもよいことは言うまでもない。

【 0 1 1 6 】

さらに、上述した配信システムでは、Java-APによる利用を制限する対象としてAPIを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、LED（Light Emitting Diode）等の移動機が備え得るものや、移動機と共働し得るUIM（User Identity Module）やSIM（Subscriber Identity Module）等の外部機器なども挙げられる。

【 0 1 1 7 】

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

【 0 1 1 8 】

次にソフトウェア資源について説明する。ソフトウェア資源としては、APIやクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Webブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

【 0 1 1 9 】

ところで、Java-APによるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限する

ことにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Java-A PのうちのトラステッドJava-A Pについてのみ、自他のJava-A Pの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

【0120】

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの2つの利用形態（利用の種類）があるから、非トラステッドJava-A Pには読み出しでしか利用されないが、トラステッドJava-A Pには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、1つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するJava-A Pが起動されている間にWebブラウザ等が起動された場合、このJava-A Pが「パケット伝送路の利用を排他的に行う」ことを許可されていないJava-A PであればWebブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているJava-A Pであればパケット伝送路を占有して使用することができる、といった制御が可能となる。

さらに、この例を変形することで、ある種のパーミッションを与えられたJa

Java-APはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたJava-APはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたJava-APはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたJava-APはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたJava-APはパケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

【0121】

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

【0122】

また、上述の配信システムでは、Java-APの実行時にJava-APの挙動を制限するようにしたが、IPサーバ装置に格納されているJarファイルにポリシー情報を内包させ、Jarファイルのダウンロード時に、移動機において、このポリシー情報とSDF中とのポリシー情報とを比較し、両者が一致しない場合には、このJarファイルに対応するJava-APを起動できないように、あるいはこのJarファイルを含むJava-APソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

【0123】

通信事業者の公開鍵は、IPサーバ装置12～14からADFに含めて移動機16に提供されるようになっていたが、これに限らず、予め移動機に格納されていてもよい。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、ROMに書き込んだ後に移動機を販売する

方法などが考えられる。

【 0 1 2 4 】

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

【 0 1 2 5 】

上述の配信システムでは、トラステッド J a v a - A P ソフトウェアの有効期限が到来したタイミングで、その有効期限を更新するための処理を開始していた。しかし、更新タイミングは上記のものに限らず、ユーザが所望する恣意的なタイミングや、毎月末 1 回等の定期的なタイミングというように、様々な態様を採用し得る。

また、有効期限の設定の仕方は、既に説明したように日時によって設定してもよいが、この他にも、例えばトラステッド J a v a - A P ソフトウェアのダウンロード時からの期間（例えばダウンロードしてから 1 ヶ月のみ使用可能というような場合）によって設定してもよいし、トラステッド J a v a - A P ソフトウェアの実行回数や実行期間によって設定してもよい。要するに、有効期限とは、J a v a - A P ソフトウェアを無制限には実行できないようにその上限を定めた情報であればどのようなものであってもよい。

例えば実行回数で有効期限を設定した場合、トラステッド J a v a - A P ソフトウェアの起動時に J A M は S D F 内のポリシー情報を参照するようになっているので、その参照回数をトラステッド J a v a - A P ソフトウェアの実行回数としてカウントしてもよい。そして、カウントした実行回数が予め定められた数に達すると、その更新処理に移行すればよい。

また、トラステッド J a v a - A P ソフトウェアが実行されている期間を累積してカウントするような手段（例えばそのトラステッド J a v a - A P ソフトウェア内にサブルーチンとして記述する等の手段）を備えていれば、実行期間によって有効期限を設定した場合にも対応できる。そして、カウントした実行期間が予め定められた時間に達すると、その更新処理に移行すればよい。

なお、上述の配信システムの説明では「トラステッド J a v a - A P ソフトウェアの有効期限」という表現を用いていたが、より厳密には、J a r ファイルそ

のものの有効期限であってもよいし、SDFそのものの有効期限であってもよいし、その両者の有効期限であってもよいことはもちろんである。

【0126】

また、上述の配信システムでは、有効期限が到来してもそれを更新できない場合、その有効期限が到来したトラステッドJava-APソフトウェアを実行禁止となっていたが、これに限らず、その有効期限経過時にトラステッドJava-APソフトウェアから非トラステッドJava-APソフトウェアに遷移させてもよい。即ち、有効期限が到来したJava-APソフトウェアは、非Java-APソフトウェアであるとみなされ、その遷移後は、非トラステッドJava-APソフトウェアとしての、より厳しい挙動を制限を受けることとなる。

【0127】

【発明の効果】

本発明によれば、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動がこのセキュリティ記述ファイルに対応するアプリケーションに許可される。したがって、多様なアプリケーションを提供することができる。さらに、権限を示す情報は管理サーバ装置からセキュリティが確保された上で端末装置へ送信されるから、権限が第三者により改竄される虞もなく、アプリケーションに対する信頼性が確保される。

【図面の簡単な説明】

【図1】 本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

【図2】 同システムに特有のADFのデータ構成を示す概念図である。

【図3】 同システムにおいて管理サーバ装置に格納されているSDFのデータ構成を示す概念図である。

【図4】 同SDFに内包されるポリシー情報の内容を示す概念図である。

【図5】 同システムを構成する移動機の構成を示すブロック図である。

【図6】 同移動機の機能構成を示す概念図である。

【図7】 同移動機がJava-APソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

【図 8】 同移動機が J a v a - A P ソフトウェアの有効期限を更新する処理の流れを示すフローチャートである。

【図 9】 同配信システムの動作を説明するためのブロック図である。

【図 1 0】 同配信システムにて配信されるリストページを示す図である。

【図 1 1】 同配信システムを構成する I P サーバ装置が格納している説明ファイルの内容を示す図である。

【図 1 2】 同配信システムにて配信される説明ページを示す図である。

【図 1 3】 同 I P サーバ装置が格納している説明ファイルの内容を示す図である。

【図 1 4】 同配信システムにて配信される説明ページを示す図である。

【図 1 5】 同配信システムを構成する I P サーバ装置 1 3 が格納している説明ファイルの内容を示す図である。

【図 1 6】 同配信システムにて配信される説明ページを示す図である。

【図 1 7】 同配信システムの動作を説明するためのシーケンス図である。

【図 1 8】 同配信システムの動作を説明するためのシーケンス図である。

【図 1 9】 同配信システムの動作を説明するためのシーケンス図である。

【図 2 0】 同配信システムの動作を説明するためのシーケンス図である。

【図 2 1】 移動機にて表示される画面を示す図である。

【図 2 2】 同配信システムの他の動作を説明するためのブロック図である。

【図 2 3】 同配信システムの他の動作を説明するためのシーケンス図である。

【符号の説明】

- 1 1 インターネット
- 1 2、1 3、1 4 I P サーバ装置
- 1 5 移動パケット通信網
- 1 6 移動機
- 1 7 ゲートウェイサーバ装置
- 1 8 管理サーバ装置

1 6 D、1 2 A、1 3 A、1 4 A、1 8 A 不揮発性メモリ

1 6 A ROM

1 6 B CPU

1 6 C 表示部

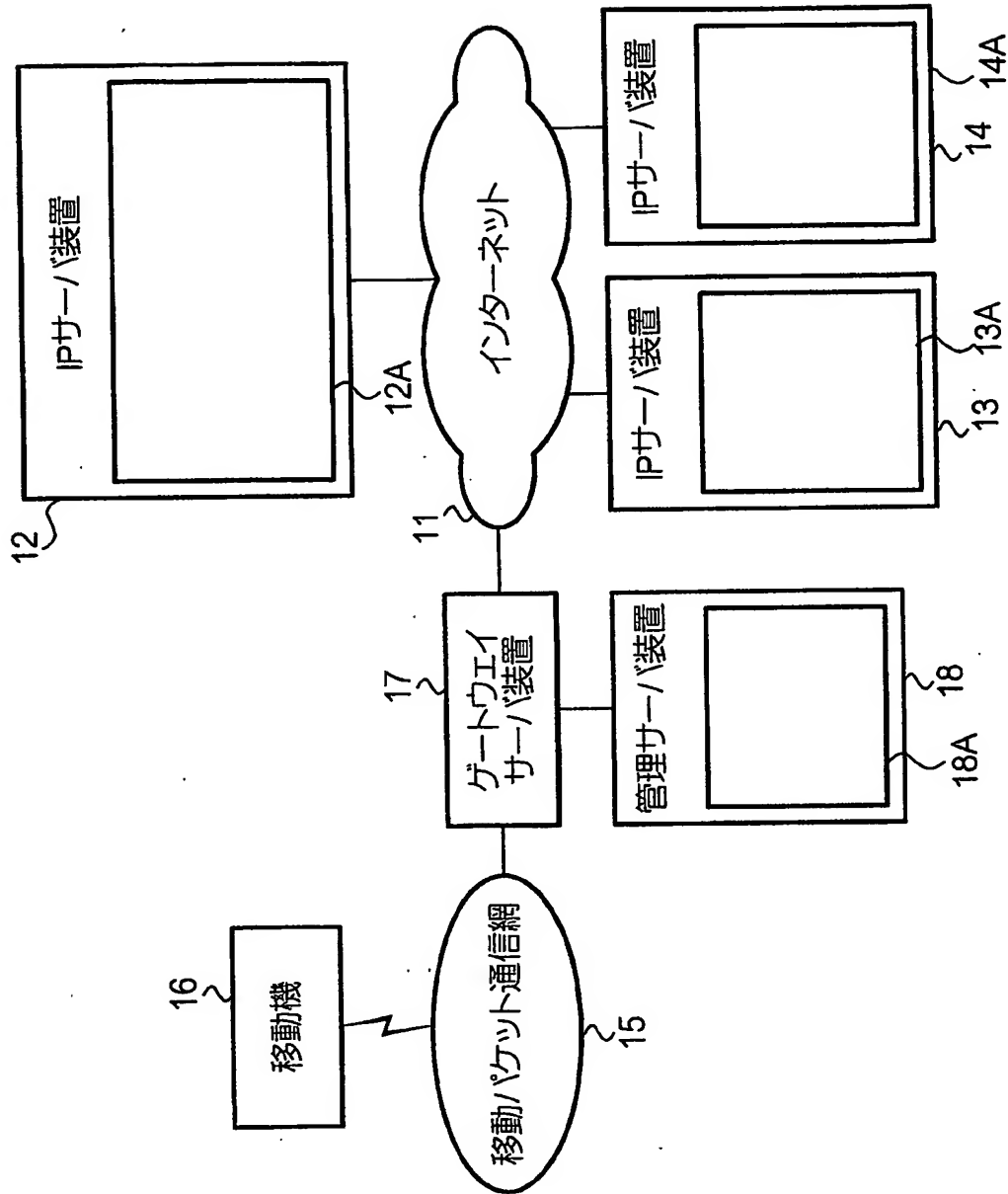
1 6 E RAM

1 6 F 通信部

1 6 G 操作部

【書類名】 図面

【図 1】



【図2】

APIID	ハッシュ値	パッケージURL	...	SDF-URL	公開鍵
-------	-------	----------	-----	---------	-----

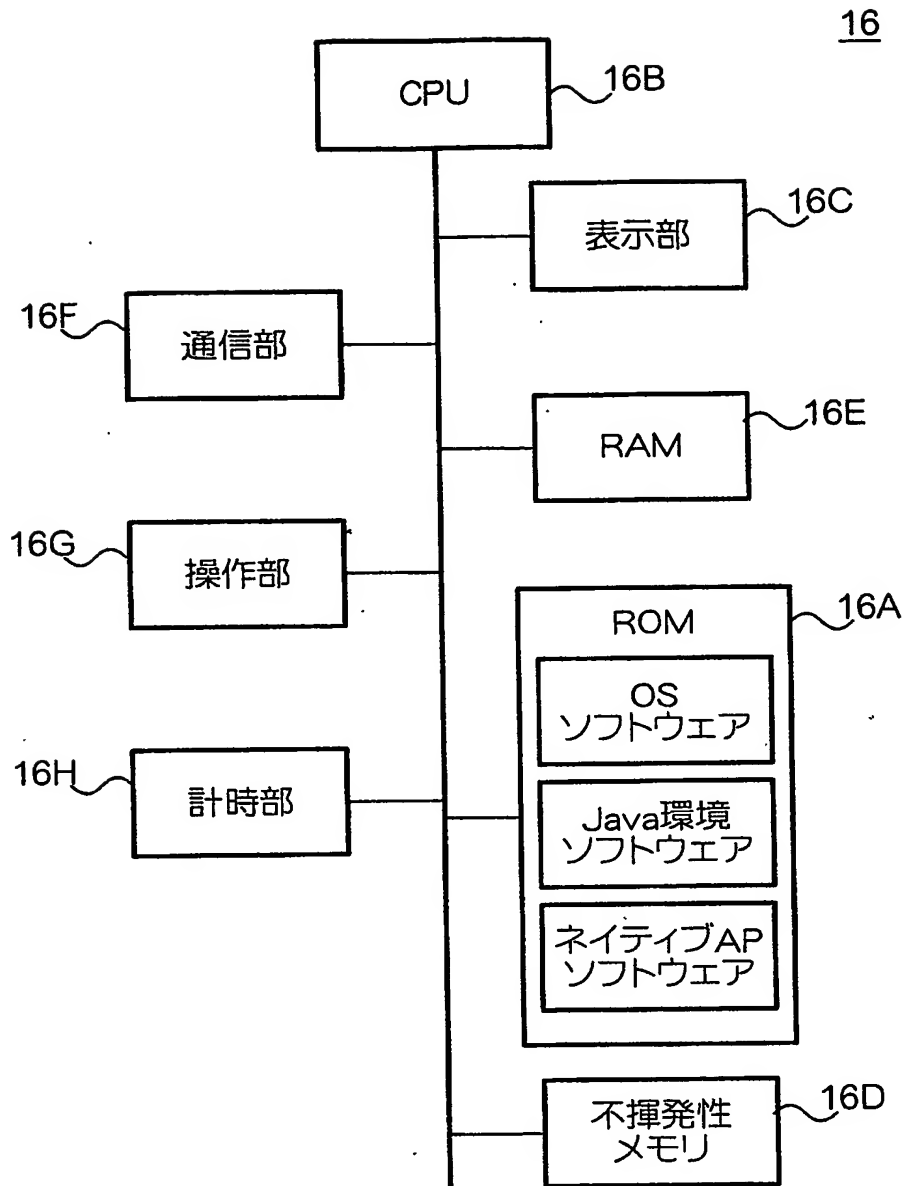
【図3】

APIID	ポリシー情報	有効期限
-------	--------	------

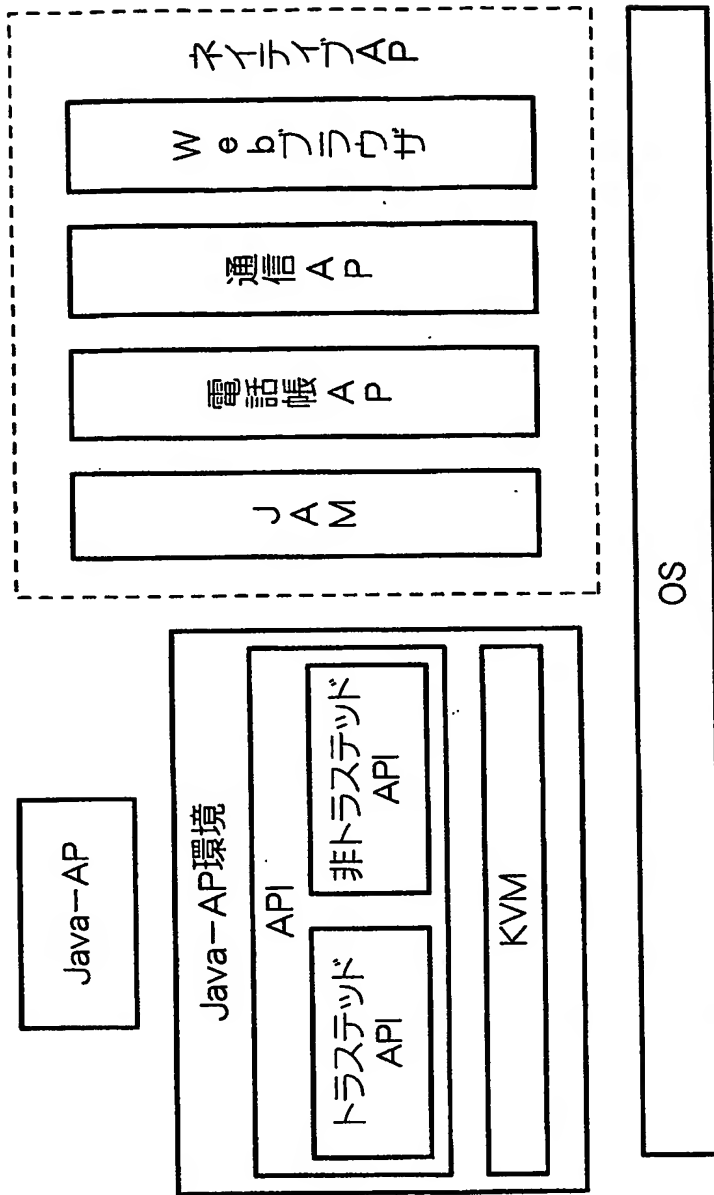
【図4】

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

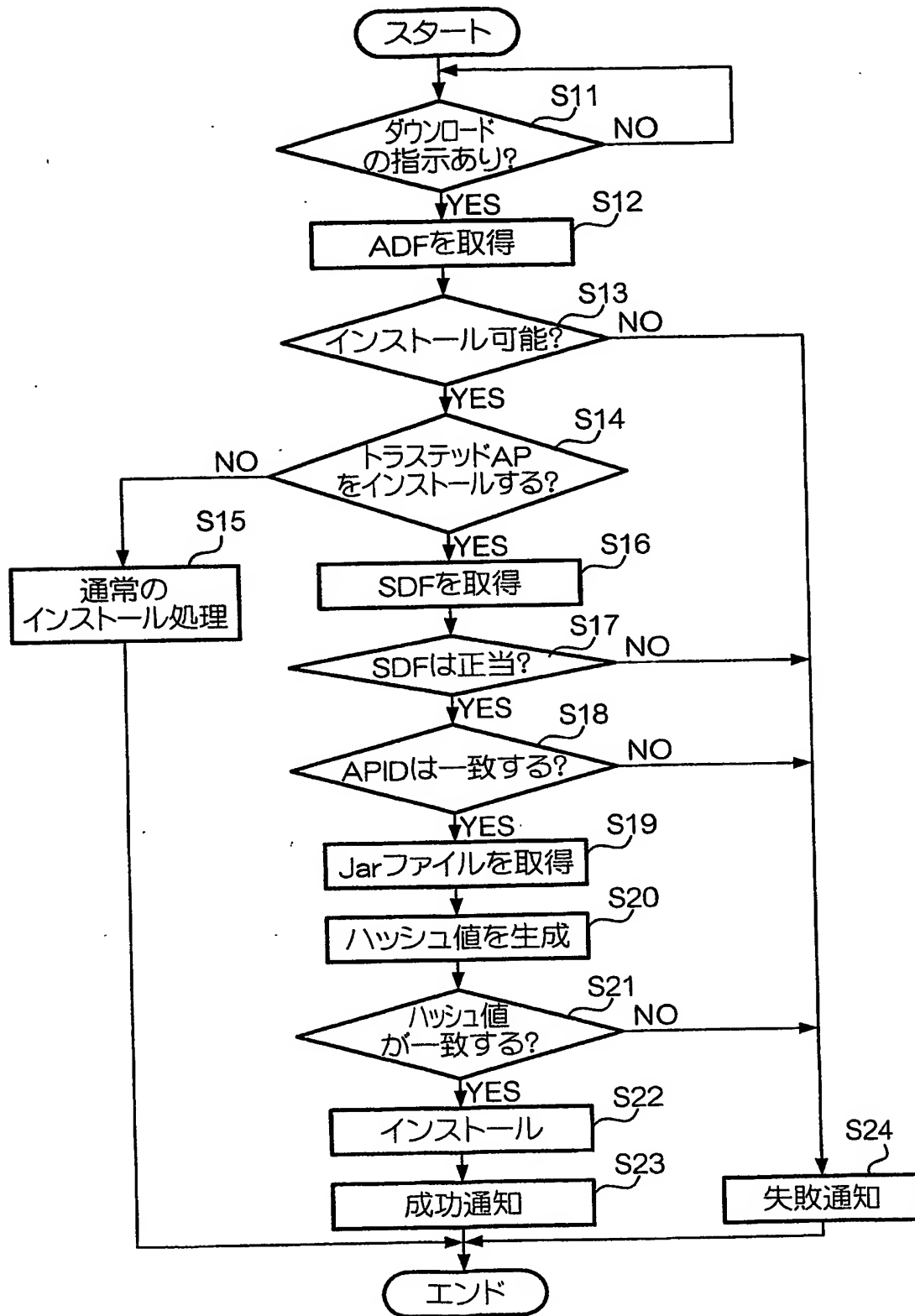
【図 5】



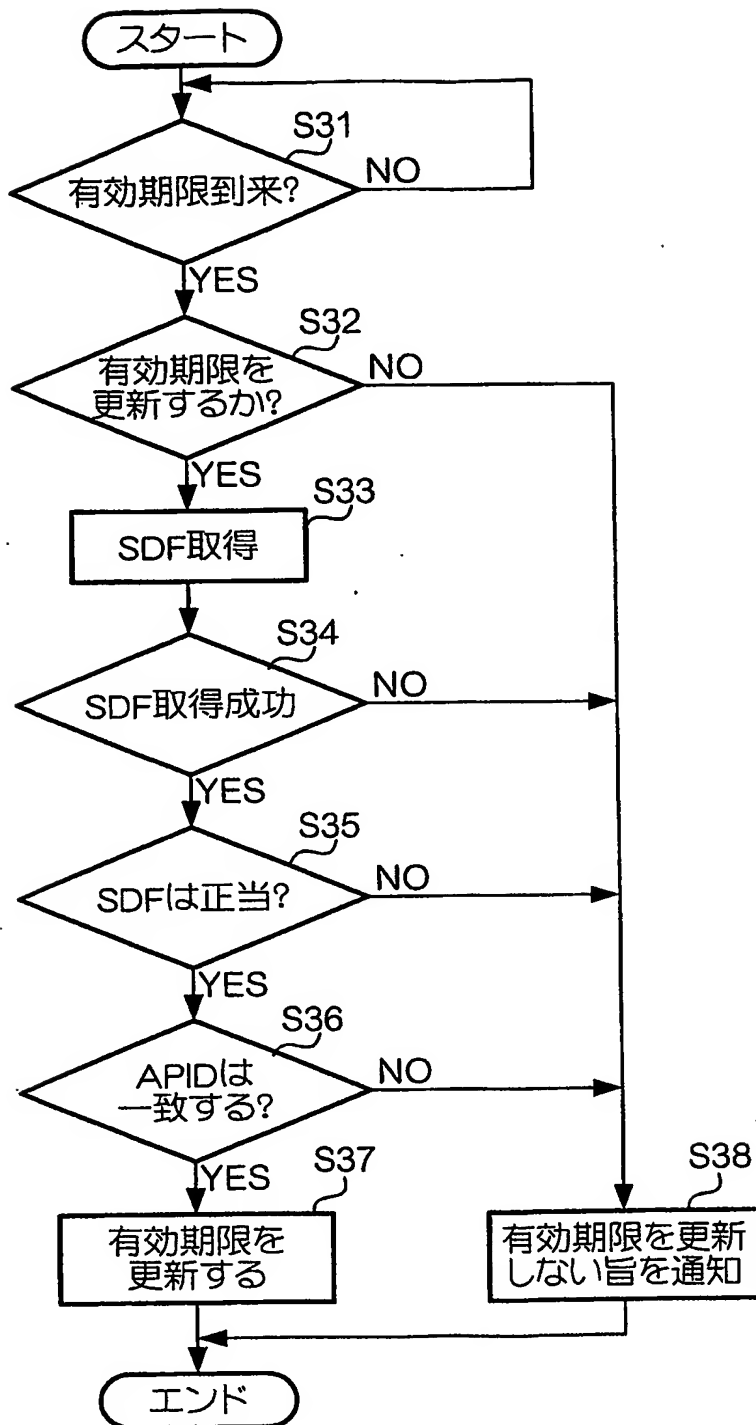
【図6】



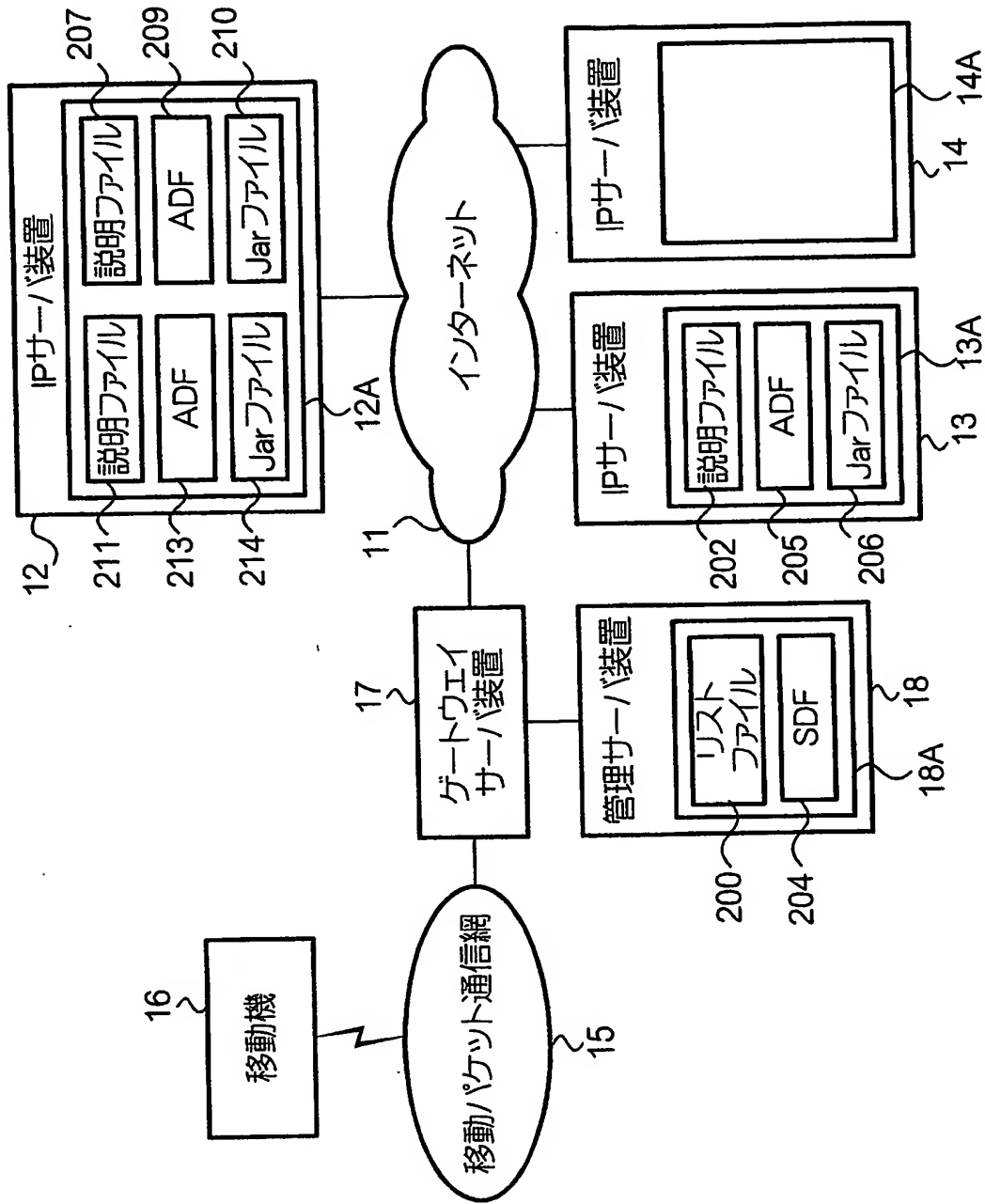
【図 7】



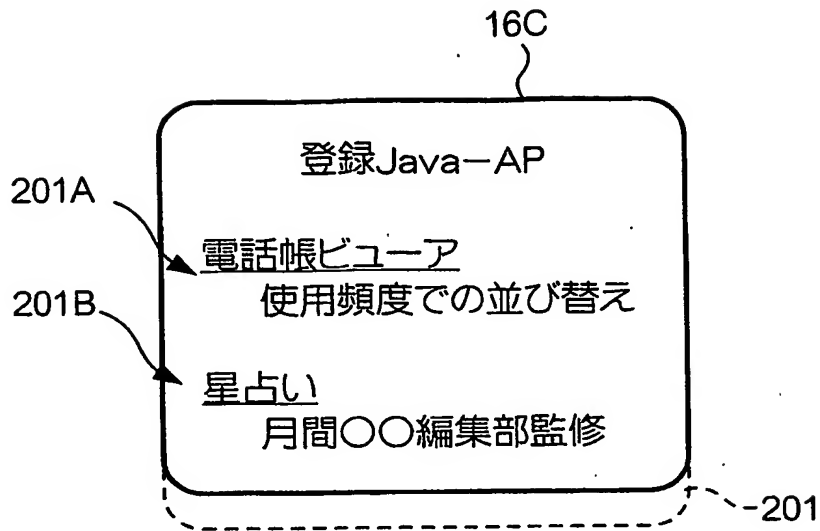
【図 8】



【図9】



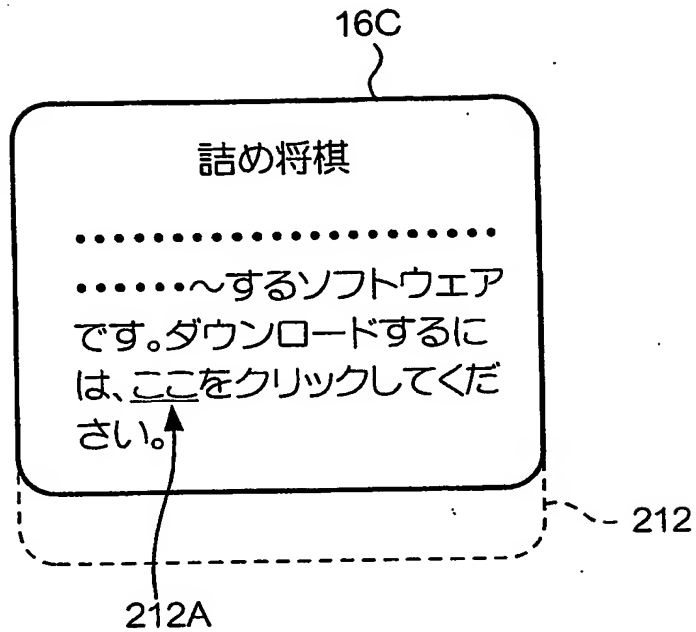
【図 10】



【図 11】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/shogi.jam">
詰め将棋
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

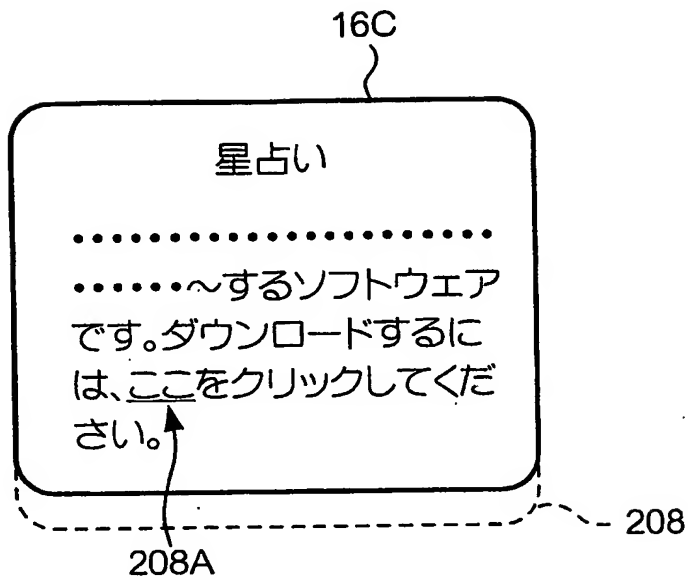
【図 1 2】



【図 1 3】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam">
星占い
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。
```

【図14】



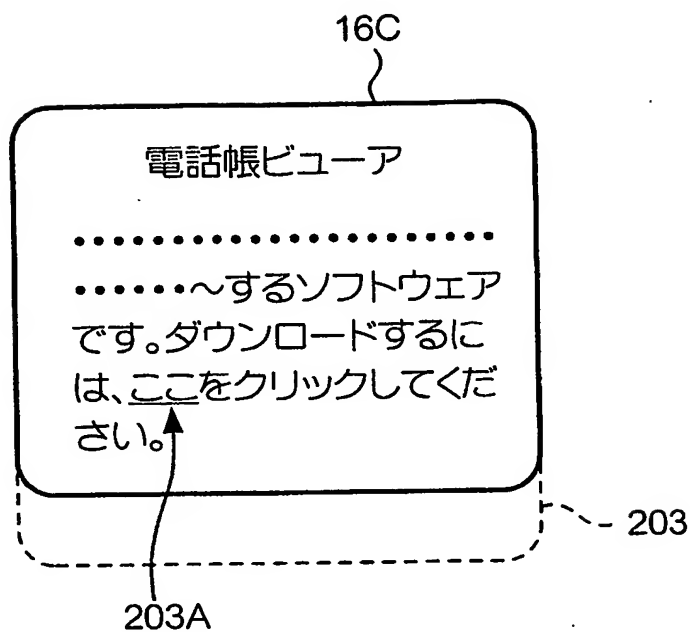
【図15】

```

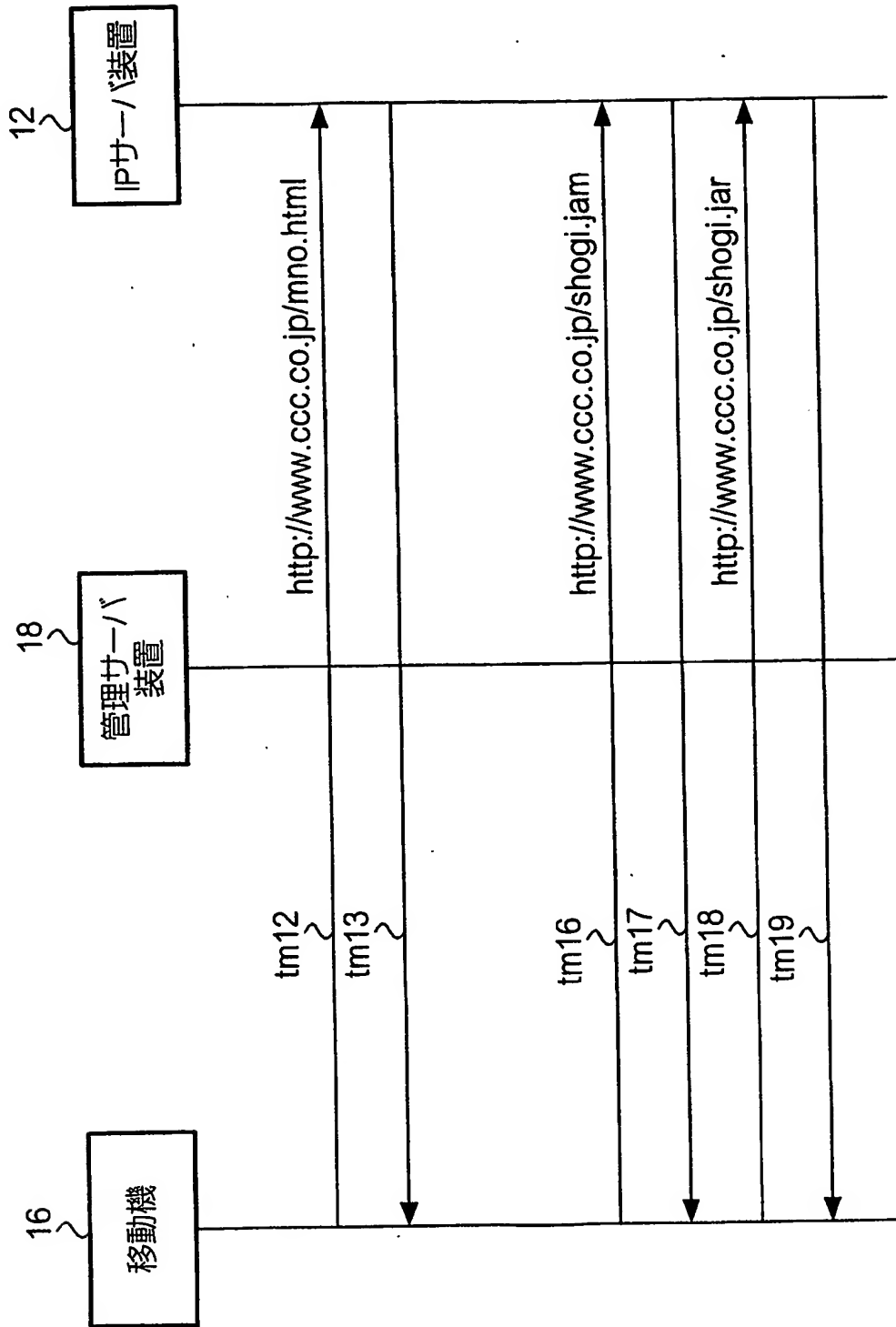
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/viewer.sdf"
type="application/x-jam">
  電話帳ビューア
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。

```

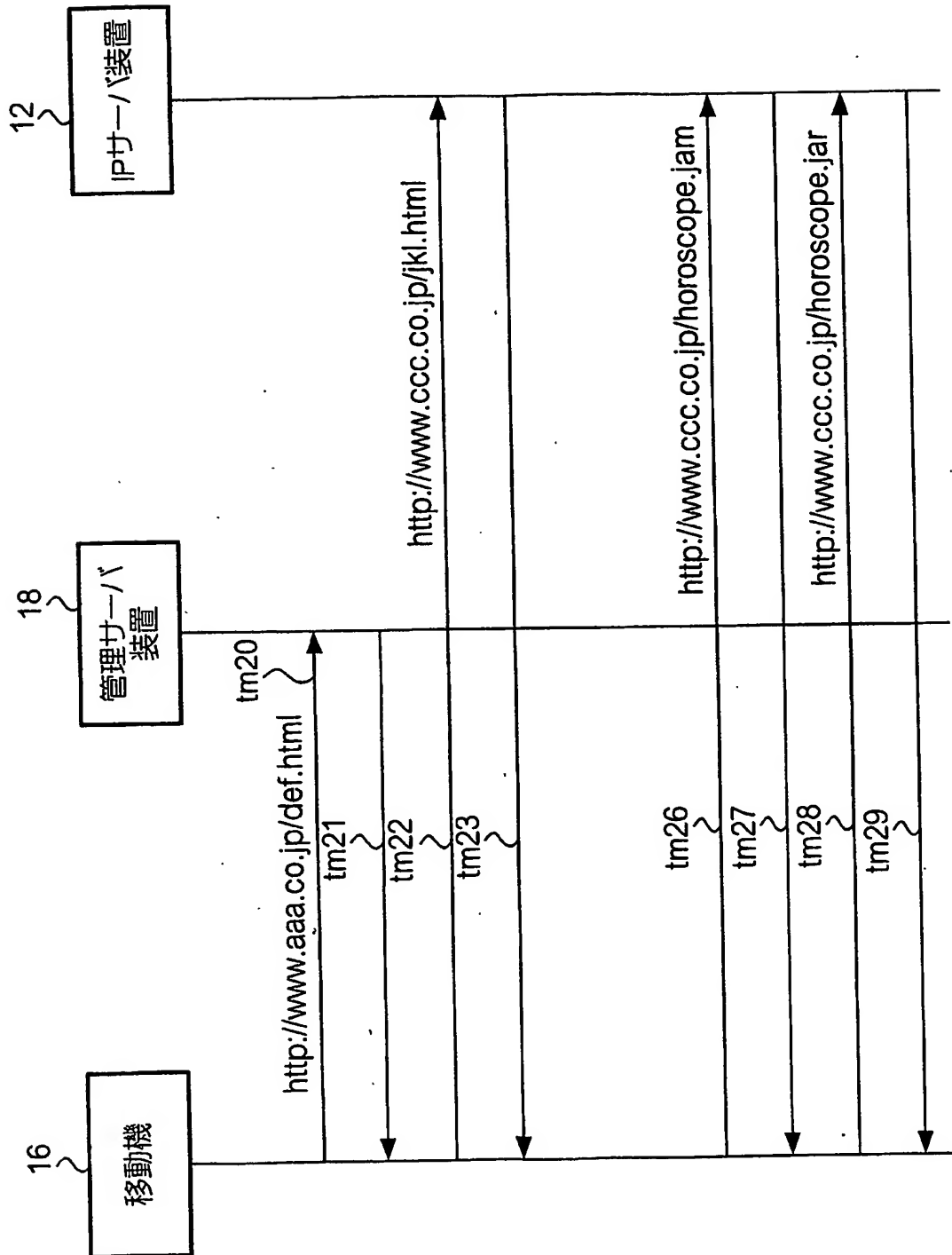
【図 16】



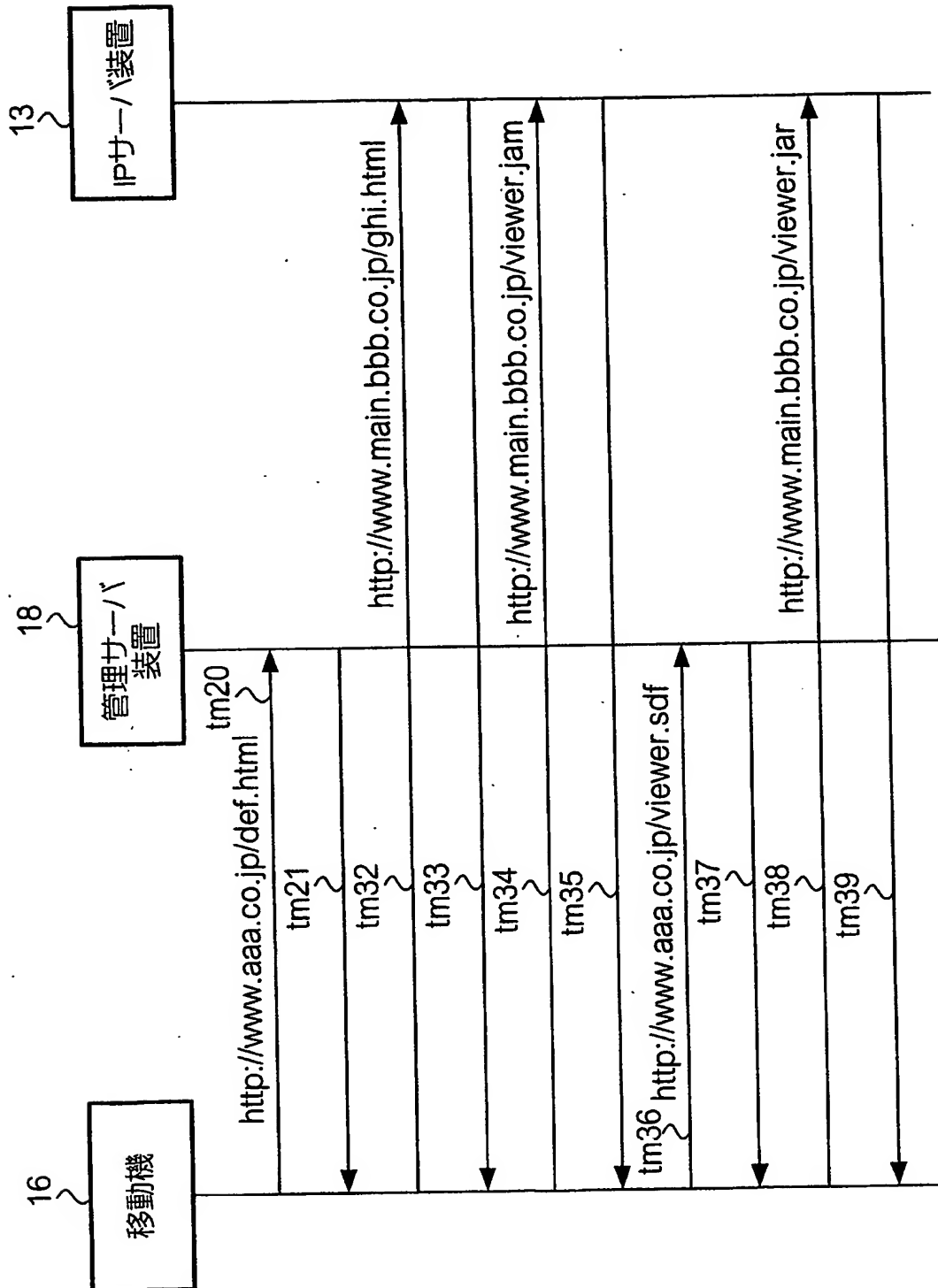
【図17】



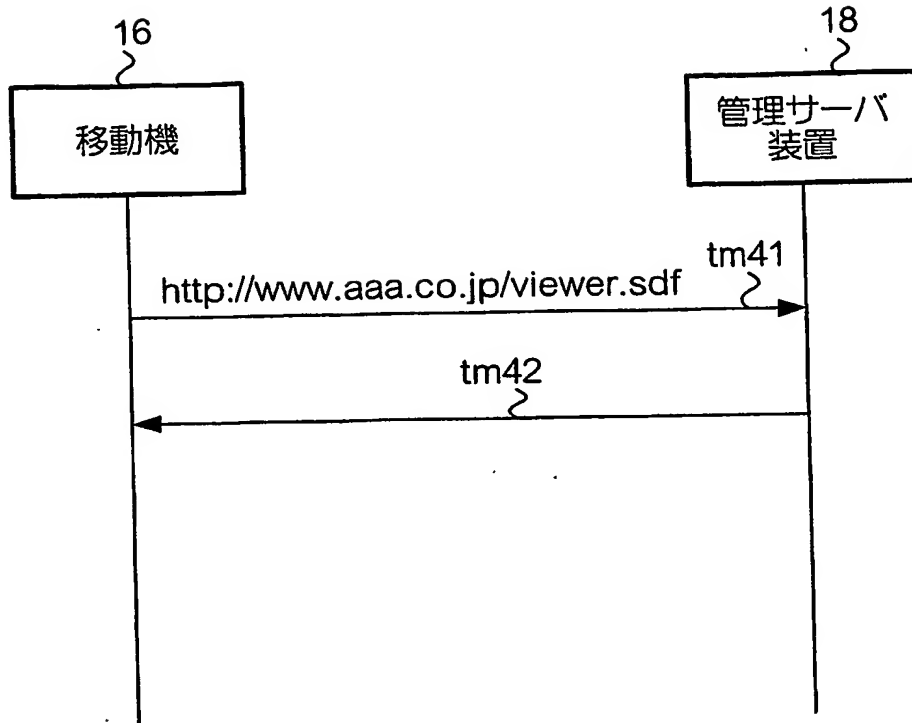
【図18】



【図19】



【図 20】



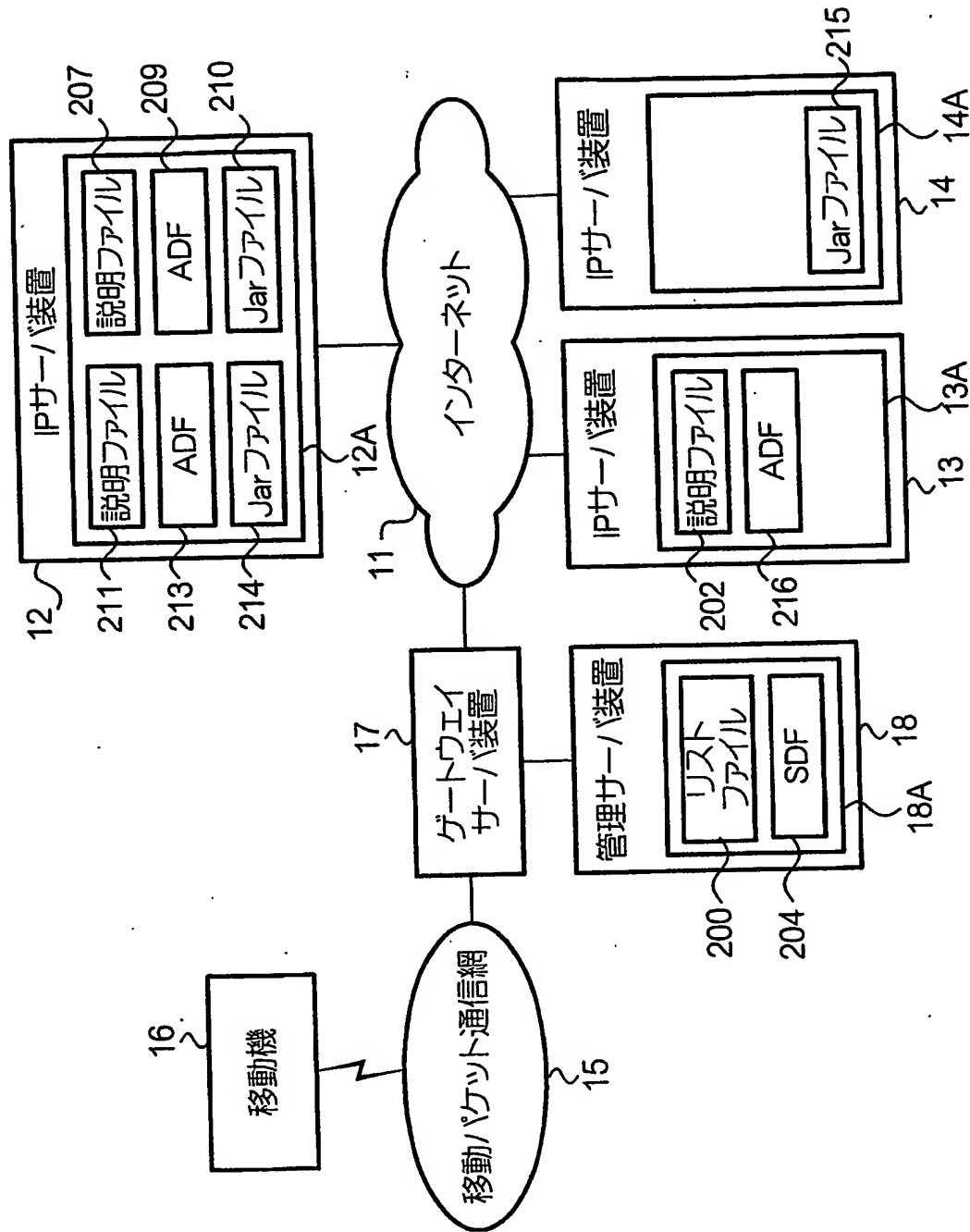
【図 21】

アプリケーション
"電話帳ビューワ"
の有効期限を更新しますか?

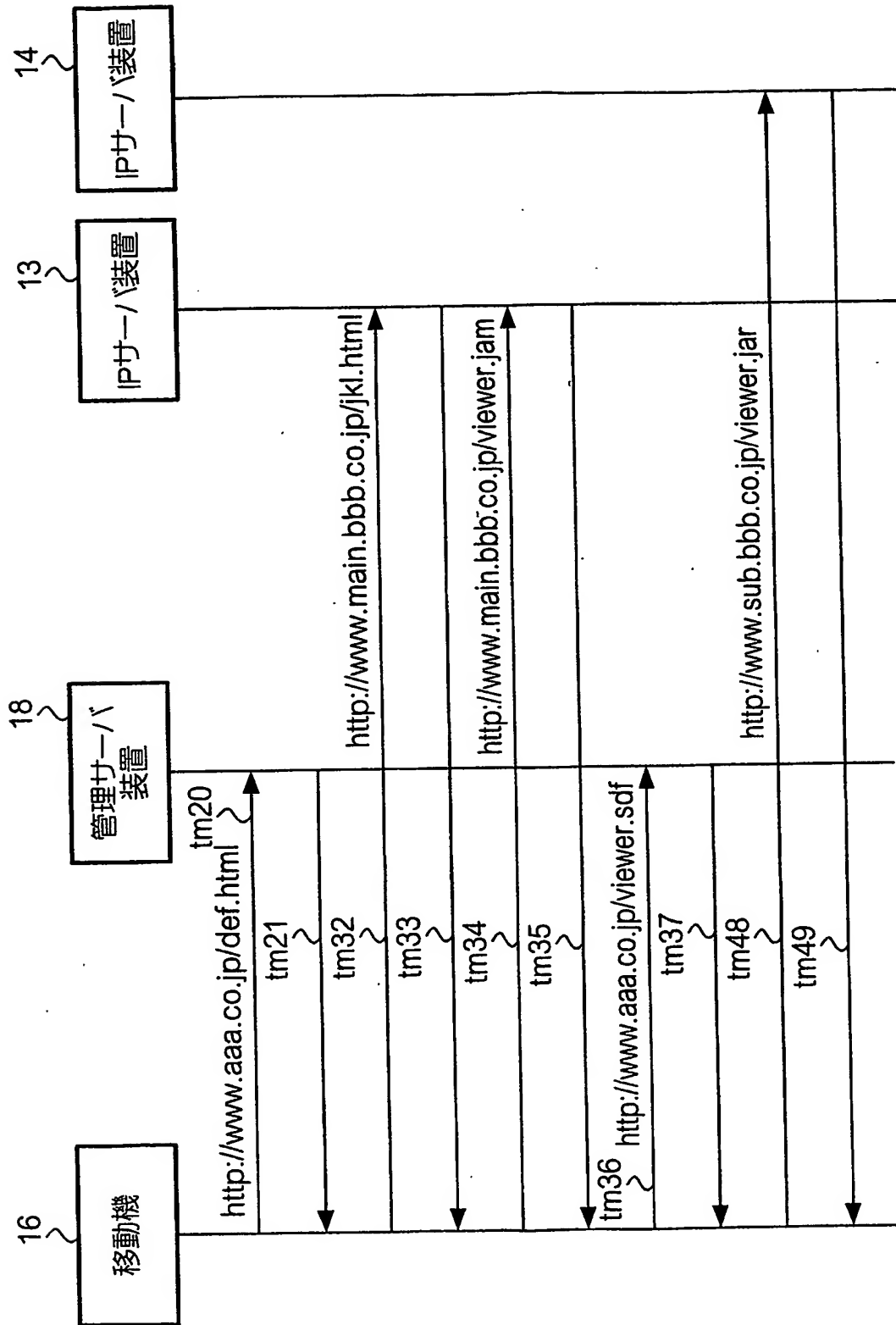
Yes

No

【図 22】



【図 23】



【書類名】 要約書

【要約】

【課題】 IPの自由度を制限することなく、信頼性の保証されたJava-AP (Javaアプリケーション) ソフトウェアを移動機へ配信する。

【解決手段】 Java-APソフトウェアを起動することができる移動機16が、IPサーバ装置13からADF205を取得し、このADF205を用いて信頼できる機関（移動パケット通信網15を管理する通信事業者）が管理する管理サーバ装置18からSDF（セキュリティ記述ファイル）204を受信し、次いで、ADF205を用いてIPサーバ装置13からJarファイル206を取得し、これらのファイルを内包するJava-APソフトウェアを自身にインストールする。このJava-APソフトウェアを起動することで実現されるJava-APは、SDF204に内包されているポリシー情報で表される権限の範囲内で動作する。

【選択図】 図9

出 願 人 履 歴 情 報

識別番号 [392026693]

1. 変更年月日	2000年 5月19日
[変更理由]	名称変更
住 所	東京都千代田区永田町二丁目11番1号
氏 名	株式会社エヌ・ティ・ティ・ドコモ